Information Assurance study

Prepared by the C4ISR Committee

NDIA

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

STRENGTH THROUGH INDUSTRY & TECHNOLOGY

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00000000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Assurance Study	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) C4ISR Committee NDIA	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 154	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

3. REPORT TYPE AND DATES COVERED
White Paper

4. TITLE AND SUBTITLE
Information Assurance Study

5. FUNDING NUMBERS

6. AUTHOR(S)
C4ISR Committee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This document entitled “Information Assurance Study” was prepared by the C4ISR Committee of the National Defense Industrial Association (NDIA). It reports the results of the NDIA study tasking summarized as follows. Because of the many concerns mentioned above, in 1998 the OASD/C3I requested that the National Defense Industrial Association (NDIA) undertake an independent study to determine if DOD/ Federal government information assurance support can be augmented through outsourcing to private industry. DOD defines outsourcing as “the process of shifting functions that are traditionally done in-house to the private sector.” This is sometimes referred to contracting out. In these cases, the workload shifts, but no government facilities are transferred to the private sector.” The Terms of Reference (TOR) for the study required that it would: Provide industry’s view of best practices that can be employed to improve the level of IA across the wide range of DOD communications. Gather statistics, analyze and catalog methods, procedures, processes and tools that have been used to support information security within DOD and industry. Investigate the expected protection requirements associated with the implementation of new systems, COTS products an

14. SUBJECT TERMS
Information Assurance

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

EXECUTIVE SUMMARY

TABLE OF CONTENTS

1. THE INFORMATION AGE

No one can argue with the impact that information has had on the entire world. The explosion of information technologies has set in motion a virtual tidal wave of constant change that profoundly affects organizations and individuals in multiple dimensions. Rapid advances in these information based technologies have thrust information into the center stage in society. Information itself has become a strategic resource vital to national security. Industry, the public sector and governments have become information age organizations. Timely, accurate and relevant information is absolutely essential to all types of operations. Today's relatively low cost of information technology (IT) and systems makes it efficient and cost effective to extend capabilities to an unprecedented number of users. The broad access to, and use of, these information systems enhances everyday functions. However, these useful capabilities induce dependence, and that dependence creates vulnerabilities. ***Welcome to the information age!***

2. CONCERNS

The Department of Defense (DOD) information infrastructure consists of more than 2 million computers, 10,000 local area networks and 1,000 long distance networks. More than 95% of DOD's systems use public communications networks available to the general public. These networks are classified as the global, national, and defense information infrastructures (GII, NII and DII). All of these networks use an interconnected transport medium linked to public switches that route data between geographically separated systems. These automated systems allow the DOD to command, control, protect, pay supply, and inform all of its organizations. As DOD's dependence on these increasingly interconnected information systems grow, so does its vulnerability.

In general, information systems for the DOD, other Federal government agencies and industry have become increasingly more vulnerable to inadvertent and covert unauthorized intrusion. These intrusions threaten the effectiveness of the systems, impact the readiness of organizations to perform their missions, and have the ability to disrupt the delivery of critical services nationwide. The concern of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) is how it will be able to provide Information Assurance (IA) against a rising threat that has the potential to outstrip available DOD resources to monitor and test current and new systems. DOD defines IA as "Information Operations (IO) that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities."

3. BACKGROUND

Since 1993, both the Congress and the DOD have recognized how critical IA has become to modern military operations. Unfortunately, also recognized was a lack of coherence among various IA plans and programs across DOD. As a result, there have been many organizations which have studied this subject including one mandated by Congress. One outstanding result of these efforts has been the establishment of a DOD-wide Information Assurance Program (DIAP). The DIAP provides for the planning, coordination, integration and oversight of DOD's IA resources to assure the availability, integrity, authentication, confidentiality and non-repudiation of DOD's mission essential and mission support information. The OASD/C3I is responsible for the DIAP and established an organization under a Director to manage the DIAP.

The strategy for achieving DOD IA is based upon the integration and coordination of the following five key elements within an overall framework:

Protection of networks and systems through the development, procurement, and application of trusted operating systems and databases, access control, and application security.

Intrusion detection and monitoring to provide prompt awareness of attacks and other irregular network activity within DOD systems.

Reaction to, and recovery from, attacks and other anomalous activities.

Measurement of the operational readiness of our information systems, networks, and infrastructures.

Education, training, and awareness.

The DOD has drafted an IA vision statement which states "By 2003, the Department of Defense will have achieved *ubiquitous, assured connectivity* across the entire Department, and will set the example for assured communications, information and business transactions for the Federal Government and industry." Vision components include:

- Unconstrained connectivity, visibility end-to-end.
- Single personal identification card with personal information, security information, etc., and access control credentials.
- Global interoperable Security Management Infrastructure which is mostly COTS based.

4. TASKING

Because of the many concerns mentioned above, in 1998 the OASD/C3I requested that the National Defense Industrial Association (NDIA) undertake an independent study to determine if DOD/ Federal government information assurance support can be augmented through outsourcing to private industry. DOD defines outsourcing as "the process of shifting functions that are traditionally done in-house to the private sector." This is sometimes referred to contracting out. In these cases, the workload shifts, but no government facilities are transferred to the private sector." The Terms of Reference (TOR) for the study required that it would:

- Provide industry's view of best practices that can be employed to improve the level of IA across the wide range of DOD communications.
- Gather statistics, analyze and catalog methods, procedures, processes and tools that have been used to support information security within DOD and industry.
- Investigate the expected protection requirements associated with the implementation of new systems, COTS products and diverse information distribution requirements. Evaluate latest DOD and industry measures to safeguard information.
- Investigate methods to improve the ability of DOD to measure and test for readiness of information systems to provide IA.
- Investigate viability, related issues and possible implementation methods to determine if Red Team testing and certification of DOD information systems could be outsourced to private industry.
- Investigate and make recommendations on possible approaches for creating an organizational process that would provide guidance for outsourcing to industry.

5. STUDY APPROACH/PROCESS/PROCEDURES

The study began in May 1998 and was supported by individuals from the following companies and organizations: Booz • Allen Hamilton, General Dynamics, Georgia Tech Research Institute, C3I, Delfin Systems, ITT Industries, MITRE, Information Management Group, SAIC, GRC International, CSC, GTE, Harris and TRW. An official from DOD's IA Directorate provided liaison and support assistance. The study team organized by assigning a lead member plus other individuals to each of the above six terms of reference. The study team gathered data by various means including reviewing documents and publications, visiting DOD organizations and military commands and units, and holding discussions with key DOD civilians and military officers, as well as with senior industry officials.

6. DOD ACTIONS AND ACTIVITIES

No one can argue with the fact that the DOD has taken the lead on IA within the government. It was bound to happen not only because of Congressional interest and pressure, but also because the military services have become so dependent on information systems. In the absence of direction from higher authority, the DOD decided to move out on IA in order to protect its people and systems. ***The catalyst for real action has been the influx of new action oriented civilian and military officials with a vision and a real sense of urgency***. They have made a difference. There is movement on all fronts. There is more IA awareness with policies and procedures being changed. New organizations have been established with their only functions being IA. Readiness, costs and risk management are being addressed. Red Teams have been active and vulnerability assessments are taking place. Tools and systems are being tested, Lessons learned and best practices are emerging. And there are more actions related to training and certification. Despite all of these activities, there are still some fundamental problems and a lot of room for improvement. These areas are discussed later in the report.

7. CONCLUSIONS

7.1 The Answer Is

The Study Team was asked to determine if DOD IA support can be augmented through outsourcing to private industry. It quickly became apparent that ***the answer is a resounding yes!*** On many fronts and in many forums, industry is currently providing IA support to the DOD.

7.2 There Is A Market for IA Services

There is a market for industry support to government IA activities including Red Teams. The government does not have sufficient manning nor expertise to conduct all such activities with internal resources. Industry, for its part, contains a large pool of experienced and qualified IA experts who could be used to augment government assets. Industry wants to participate and looks forward to the opportunities and challenges that such efforts hold. However, the effort must make sense from a business perspective.

7.3 Industry Will Participate

Industry is interested in providing IA services to the government provided that certain issues are addressed adequately. These include but are not limited to:

Contractual limitations and constraints
Legal liability and indemnification
Long term commitment to justify investments in personnel, training and equipment
Consent
Continuity of effort

7.4 Red Team Activity Can Be Outsourced

While the government certainly needs to maintain control at every level as well as establishing policy, guidance and control functions, nearly all Red Team activity can be outsourced to industry.

7.5 Government Needs Industry Support

Industry support of and participation in IA activities is essential if the government hopes to be successful. There are simply insufficient internal government assets (both in breadth and depth) to adequately perform all required IA activities in any reasonably aggressive program.

7.6 Policy and Architecture Are Lacking

There is no commonly accepted DOD policy and architecture which covers all aspects of IT/IA. While there continues to be active attempts to fully establish such a policy and architecture, the goal hasn't yet been achieved. In the absence of a guiding policy and architecture, individual agencies, offices and military units continue to move forward taking individual actions to deal with IT/IA. Often there is duplication of efforts and it difficult to measure effectiveness in many areas. This lack of a policy and architecture is particularly apparent when it comes to dealing with industry participation in IT/IA activities. We could not find any evidence of any high level policy or architecture which governs outsourcing IA support to industry.

7.7 DOD IT/IA Organization Is Lacking

DOD is not properly organized to deal with the most important aspects of IT/IA/IO. There is no focal point with proper authority which can ensure commonality, synergy, standardization, responsiveness, awareness, training, staffing, testing, certification and budgeting across all of DOD to include the military services. We could not identify any single organization which has responsibility for dealing with outsourcing IA support to industry.

7.8 Costs Must Be Measured And Managed

Cost have to be managed by both government and industry. An acceptable way to measure return on investment must be established and agreed upon by all participants. The government needs to be fully aware of what services they are buying and industry has to be able to show that IA activity is a worthwhile business. Within the government, return on investment (ROI) needs to be calculated with more than accounting practices in mind. The observed practices of accounting for work done by government employees as "free goods" can lead to financially flawed decisions. ROI is a potentially useful tool for government agencies but appears to be essentially incompletely implemented.

7.9 There Are Legal, Liability, And Contractual Considerations

Legal issues are equal to, if not greater than, the management issues. Many issues must be addressed in order to ensure that outsourcing continues to be an asset which can be used. Current laws in the areas of computers, software, networking, information privacy and the liability issues associated with each, are only just beginning to be tested. It is almost certain that reevaluation of existing laws will be required as issues related to IA activities arise. We do not believe that the DOD has put enough emphasis on legal issues related to outsourcing IA functions. As a result, both government and industry organizations, as well as individuals involved in carrying out certain IA responsibilities, are being exposed to legal risks which could pose significant problems.

7.10 Risks Must Be Managed

Some level of risk is unavoidable. Considering the technology available today, it is unlikely that a completely “bullet proof” system could be built and even if it could, the cost would be prohibitive. Therefore risk must be evaluated, assessed, and managed within the constraints of operational readiness and budget allocations.

7.11 Information Flow Is A Concern

Information does not appear to flow well throughout the DOD. Many agencies and organizations do not always receive important information related to directives, required corrective actions, best practices, test results, industry alerts, etc. One example previously mentioned was that many DOD system administrators were not aware of a new commercial software upgrade which corrected a serious security problem. Another example was that many key senior ASD/C3I officials were not aware of this Study despite a Letter of Introduction from the Senior ASD/C3I Civilian who directs that office.

7.12 Inventory Of IT/IA Activities

For available information, it appears that the DOD is not fully aware of what IT/IA activities are being performed and by whom across its entire organization. Although there are many reasons for this, the primary cause is that both civilian and military personnel in non-IT/IA career fields are performing ill-defined IT/IA functions part-time. This is particularly significant because it makes it very difficult to determine who has access to DOD’s information infrastructures. It also appears that the DOD is unable to identify the number of industry/contractor personnel currently being used to carry out/support IT/IA functions.

7.13 Common IT/IA Language/Terminology

In several areas, the DOD has attempted to develop definitions that accurately reflect today’s IT/IA activities. While this is a good start, it must go further and address all IT/IA activities in all areas. This standardization would go a long way to preventing one organization of having a totally different understanding of a term from another organization.

7.14 Red Team Training And Certification

Red Teams are being used more frequently across all of the DOD and it appears that this usage will continue to increase. Their successes have varied depending on any number of reasons from access to people, processes and data, to acceptance by authorities, to capabilities/experience of team members. Industry has participated in these Red Teams and this support will also continue to increase. It is imperative that all people involved (government and industry) are properly trained and certified. Common training and certification standards should be established to include minimum and maximum timeframes to accommodate rapid changes in technology.

7.15 Readiness

IA is now accepted as a readiness criteria. However, there are still several “loose ends” that the DOD has to address. First and foremost is a widely accepted definition of IA readiness. Next is how to measure and test for the readiness of information systems to provide IA. And lastly is how to report IA readiness. There are several DOD organizations working on this subject. However progress continues to be slow. In the meantime other DOD organizations, particularly the military services are adopting their own ways and means to deal with this issue. We believe that the DOD has to quickly define what constitutes IA readiness and standardize readiness measurement metrics and IA readiness reporting.

7.16 COTS

IT/IA COTS products are becoming more numerous and cheaper. The use of these products by the DOD will continue to increase. This usage causes concern and officials are asking to what extent can they trust COTS products. We found that there are many initiatives underway in the DOD to test and evaluate these products. While we applaud these efforts, we found that there is no DOD central management, focus or direction. Dedicated people and organization are doing their own thing, often marching to a different drummer. We believe that direction, focus and management has to be implemented ASAP. Results of all actions must be shared so that all concerned are aware of risks. Also, DOD and industry should establish an open and trusting partnership to deal with COTS products.

7.17 Best Practices And Tools

Great amounts of information related to IT/IA best practices and tools is available from many sources. The numbers taken together are in the hundreds. Both the DOD and industry could learn a lot from this information. The major problem is how to assemble, keep track and make available all of this data. We could find no DOD organization which has this responsibility. As a result, each agency, office or military unit is left to their own discretion. This lack of synergy hampers efficiency, results in duplication, and can increase risks and vulnerabilities. Someone or some organization should take charge.

8. Recommendations

8.1 Policy And Architecture Must Be Established

DOD gives every indication that IA is a top priority. The Study Team agrees with this philosophy. If this is the case, then DOD must continue its efforts to establish a definitive IA policy and architecture which identifies roles, responsibilities, accountability, reporting responsibilities, etc. This policy and architecture should be established at a high DOD level and be acceptable to all DOD civilian and military organizations. If the development of this overall policy and architecture continues to lag, then we strongly recommend that DOD develop a policy and architecture which contains provisions that will allow the government and industry to continue to participate in IA activities. This should include the outsourcing of IA functions to industry. We also recommend that the DOD continue its efforts to integrate and consolidate Pentagon and OSD IT.

We believe that DOD must move toward a longer range view and get away from short-term and quick-fix scenarios that it finds itself dealing with on many occasions. A well thought-out architecture with a realistic, funded, and high priority plan of action and milestones (POA&M) is highly desired.

8.2 Organizational Concept

DOD should adopt an organizational concept similar to the Information Assurance Center (IAC) previously described in Section 2.6.1. The best opportunity for success most probably takes the form of a brand new, high level, totally independent, IA specific organization with direct access to the Secretary of Defense and with authority for direct liaison with all external federal government departments, agencies and organizations. We view this organization to be a “focal point”/ “clearing house”/ “one-stop shopping center”/ “data warehouse” for IA activities. Some existing IA related organizations should report to this new entity or be absorbed by it.

We agree with a DOD official who recently recommended the following: that the DOD appoint an IO integrator for all of the military services to ensure that synergy is achieved, redundant parallel efforts are eliminated, and suboptimization is detected: otherwise efficiencies will not be realized, and “risks accepted by one, will be shared by all.” We believe that the organizational concept we are recommending could assume this and other similar types of responsibilities for all of DOD.

8.3 Legal, Liability And Contractual Considerations

Section 2.5.2 of this study contains an extensive discussion of legal issues ranging from how IA support can be outsourced to industry to how to cover participants from liability exposure. The following recommendations are as a result of that specific effort:

When conducting IA and Red Team Activities, the DOD assumes the risk of damaging its equipment and facilities, and possible liability to its employees and third parties. The DOD should provide the appropriate levels of liability protection to contractors by virtue of acting in the government stead.

In support of IA and Red Team activities, contractors may technically violate some laws associated with the improper use of telecommunication resources, computer security, or other protected areas. The government should provide some level of immunity against prosecution for these violations.

IA and Red Team outsourcing requires careful definition and government approval of the Statement of Work (SOW). A well written SOW helps to define the activity for insurers and may allow contractors to claim the protection of the government contractor defense against tort claims made by third parties.

Non-Disclosure Agreements (NDA) should be strictly enforced to prohibit the release of any information obtained or generated during IA and Red Team activities. Further, the government should require the contractor to have each employee supporting IA and Red Team activities, execute an individual NDA to provide an additional level of confidentiality.

The SOW should have a clearly defined set of procedures for the reporting of illegal activities. These procedures should provide the contractor with guidance for additional reporting obligations (e.g. law enforcement authorities).

8.4 Best Practices

Both the DOD and industry can learn a lot from each other's best practices. (Best practices cover a wide range of activities including methods, procedures, processes, etc.) There is an incredible amount of information available that can greatly enhance overall IA operations and efficiencies. The problem is how to gather and keep track of all of this data. We recommend that the DOD task one of its organizations or support contractors with this responsibility. (If the IAC organizational concept described above is adopted, then that organization should carry out this task.) Taking inventory of best practices within the DOD and the rest of the federal government should be the top priority. A great deal of this information is readily available at various organizations' web sites. Identifying industry's best practices should come next. If industry resists, then DOD should first work with its current contractors and insist that they share their best practices within the scope of their existing contracts. The DOD should establish procedures to protect those industry best practices which have an economic advantages with regard to one company versus another. The compilation of best practices from government and industry will do no good unless it gets to the appropriate people and organizations in a timely manner.

8.5 Tools

What was recommended for best practices in Section 3.2.4 above pertains to tools as well. DOD must get a handle in this area because of the rapid proliferation of tools related in IT/IA and information security. There are literally hundreds of tools available and a lot of them are being used throughout DOD without any central management or focus. The following are but two examples which emphasize this point: one recent DOD IA publication identified 44 anti-virus tools; and the Navy's Information Security (INFOSEC) Web Site provides lists of tools, products and vendors that number over 200. Without a DOD focal point, valuable information on the latest in technology developments, usage experience and lessons learned can be lost or not made available to those who need it the most.

8.6 Commercial Off-The-Shelf (COTS) Products

The use of COTS products for DOD's IA activities is here to stay. The concern over the security of these products is now more widely known throughout DOD and industry. We commend the many initiatives related to testing and security enhancements now underway or in place. However, as is the case in other areas, there is no central management, focus or direction for these efforts. We recommend that DOD assign this responsibility to one of its organizations. Results of all actions must be shared so that all authorities are made aware of risks to their assets, systems, and missions and what mitigation is available.

8.7 Readiness

DOD has a real challenge on its hands as it attempts to find the ways and means to measure and test for readiness of information systems to provide IA. While much work has been done in this area, we could not find a widely accepted definition of IA readiness. Nor could we find that readiness measurement metrics have been standardized throughout the DOD. As a result, it is very difficult to measure DOD IA readiness. This in turn questions the ability of DOD units to deter anyone from exploiting vulnerabilities. We recommend that DOD continue its efforts to define IA readiness, standardize readiness measurement metrics, and IA readiness reporting. To ensure success, we also recommend that DOD devote adequate fiscal and personnel resources to these efforts.

8.8 Red Team Training And Certification

DOD is using Red Teams more and more to identify IA vulnerabilities, and to test and improve the readiness of its components. The DOD has established guidance and promulgated methodologies for Red Teaming activities. We recommend that this guidance and methodologies become standard practice and are strictly enforced.

DOD officials have stated that information superiority depends on a properly trained workforce. However, DOD has also declared that IA training and certification is a serious problem area with many vulnerabilities. We recommend that the DOD:

Establish and promulgate common IA training standards

Establish minimum training requirements for key IA personnel such as System Administrators and others before they assume their responsibilities

Establish a process to provide initial skill training to all members of the IA workforce

Establish a program for continuing IA training to maintain currency with changing technology

Establish and promulgate common IA certification standards and a process to achieve certification for both government and industry personnel.

Ensure that adequate fiscal and personnel resources are devoted to IA training and certification.

8.9 Costs

DOD is devoting a significant amount of resources to IA. As a result, a number of involved officials have proclaimed that there have been significant improvements. And while specific examples can be identified, there is no accepted measurement to determine if the results were worth the cost. As IA activities continue to expand, and as industry participation continues to increase, measuring returns on cost investment will continue to be a high priority concern. We recommend that DOD and industry join forces to take advantage of work that has already been done and identify those tools and procedures which will automate and simplify the evaluation of return on cost investment.

8.10 Risk Management

Because 100% protection of information is not possible all of the time, risk management rather than risk avoidance is necessary. Risk management addresses the enduring question of “how much security/assurance is enough?” A key task in getting the answer is evaluating current assurance status/posture (i.e. measuring IA readiness). Effective risk management must support DOD agencies and military units by orienting on what is important - mission and operations. We recommend that DOD develop and acquire risk management tools and utilize a risk management process (similar to the model described in Section 2.7.3).

It appears that IA support will continue to be outsourced to industry. The feasibility of conducting risk management on an outsourcing basis will be influenced by important constraints and factors generated by the nature of the process and by the organization’s environment. We believe that industry can perform certain risk management functions. We recommend that DOD use a risk management process to identify and select those areas where industry can provide this type of support.

8.11 Information Flow

Ensuring that the right people get the right IA information in a timely manner is a big challenge. Government and industry personnel must be more aware of vulnerabilities and their implications. DOD has faced similar information challenges in the past and designed methods to solve these problems. We recommend that DOD foster better communications through as many means as possible having a focal point assigned this responsibility would greatly enhance this effort.

9 Miscellaneous Recommendations

9.1 Common IT/IA Language/Terminology

DOD should develop and promulgate a common and acceptable IT/IA language and terminology

9.2 Inventory IT/IA Activities

DOD should determine precisely what IT/IA activities are being performed and by whom (government civilian and military, and industry) throughout its entire organization. Until this is accomplished, and IT/IA baseline is not possible.

OUTLINE

Executive Summary

Report On Outsourcing DOD Information Assurance Support To Private Industry

Appendix A - Study Terms of Reference

Appendix B – Best Practices of Leading Organizations

Appendix C – Examples of Information Assurance Tools

Appendix D – Excerpt from the Report of Defense Science Board Task Force

Appendix E – Red Team Evaluation and Acceptance Criteria

Appendix F – Red Team Life Cycle Management

Appendix G – Interview Comments

Appendix H – References and Links

Appendix I - Acronyms

Appendix J – Study Team Membership

Appendix K - Acknowledgements

Report On
Outsourcing DOD
Information Assurance Support
To Private Industry

August 1999

Prepared for ASD(C3I)

by

NDIA

TABLE OF CONTENTS

1. INTRODUCTION

This section reviews relevant current and background information related to DOD IA activities. The tasking for the National Defense Industrial Association (NDIA) study is described as well as study processes, procedures and approach.

1.1 The Information Age

No one can argue with the impact that information has had on the entire world. The explosion of information technologies has set in motion a virtual tidal wave of constant change that profoundly affects organizations and individuals in multiple dimensions. Rapid advances in these information based technologies have thrust information into the center stage in society. Information itself has become a strategic resource vital to national security. Industry, the public sector and governments have become information age organizations. Timely, accurate and relevant information is absolutely essential to all types of operations. Today’s relatively low cost of information technology (IT) and systems makes it efficient and cost effective to extend capabilities to an unprecedented number of users. The broad access to, and use of, these information systems enhances everyday functions. However, these useful capabilities induce dependence, and that dependence creates vulnerabilities. ***Welcome to the information age!***

1.2 Concerns

The Department of Defense (DOD) information infrastructure consists of more than 2 million computers, 10,000 local area networks and 1,000 long distance networks. More than 95% of DOD’s systems use public communications networks available to the general public. These networks are classified as the global, national, and defense information infrastructures (GII, NII and DII). All of these networks use an interconnected transport medium linked to public switches that route data between geographically separated systems. These automated systems allow the DOD to command, control, protect, pay supply, and inform all of its organizations. As DOD’s dependence on these increasingly interconnected information systems grow, so does its vulnerability.

In general, information systems for the DOD, other Federal government agencies and industry have become increasingly more vulnerable to inadvertent and covert unauthorized intrusion. These intrusions threaten the effectiveness of the systems, impact the readiness of organizations to perform their missions, and have the ability to disrupt the delivery of critical services nationwide. The concern of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) is how it will be able to provide Information Assurance (IA) against a rising threat that has the potential to outstrip available DOD resources to monitor and test current and new systems. DOD defines IA as “Information Operations (IO) that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.”

1.3 Background

Since 1993, both the Congress and the DOD have recognized how critical IA has become to modern military operations. Unfortunately, also recognized was a lack of coherence among various IA plans and programs across DOD.

The 1997 DOD Authorization and Appropriations Acts required a report and plans for information security. Program Decision Memorandum II (PDM-II) of 9 October 1996 directed the OASD/C3I to provide a comprehensive assessment of DOD IA programs to the Deputy Secretary of Defense (DEPSECDEF) by 31 March 1997. In response to that tasking, the Director, National Security Agency (DIRNSA) established a DOD-wide IA Task Force on 27 November 1996. That Task Force issued its report on 28 march 1997. Its overall assessment was that the IA posture of the DOD was barely adequate. The Task Force identified ten major problems under the categories of Technical, Environment, Management, and Acquisition Process. It also recommended a comprehensive approach to bring visible coherence and integration to the DOD's IA activities.

The work of that Task Force, coupled with the efforts of many other DOD organizations, has resulted in the establishment of a DOD-wide Information Assurance Program (DIAP). The DIAP provides for the planning, coordination, integration and oversight of DOD's IA resources to assure the availability, integrity, authentication, confidentiality and non-repudiation of DOD's mission essential and mission support information. The OASD/C3I is responsible for the DIAP and established an organization under a Director to manage the DIAP.

The strategy for achieving DOD IA is based upon the integration and coordination of the following five key elements within an overall framework:

Protection of networks and systems through the development, procurement, and application of trusted operating systems and databases, access control, and application security.

Intrusion detection and monitoring to provide prompt awareness of attacks and other irregular network activity within DOD systems.

Reaction to, and recovery from, attacks and other anomalous activities.

Measurement of the operational readiness of our information systems, networks, and infrastructures.

Education, training, and awareness.

The DOD has drafted an IA vision statement which states "By 2003, the Department of Defense will have achieved *ubiquitous, assured connectivity* across the entire Department, and will set the example for assured communications, information and business transactions for the Federal Government and industry." Vision components include:

Unconstrained connectivity, visibility end-to-end.

Single personal identification card with personal information, security information, etc., and access control credentials.

Global interoperable Security Management Infrastructure which is mostly COTS based.

1.4 Tasking

For the above reasons, in 1998 the OASD/C3I requested that the NDIA undertake an independent study to determine if DOD/ Federal government information assurance support can be augmented through outsourcing to private industry. DOD defines outsourcing as " the process of shifting functions that are traditionally done in-house to the private sector." This is sometimes referred to contracting out. In these cases, the workload shifts, but no government facilities are transferred to the private sector." The terms of reference for the study required that it would:

Provide industry's view of best practices that can be employed to improve the level of IA across the wide range of DOD communications.

Gather statistics, analyze and catalog methods, procedures, processes and tools that have been used to support information security within DOD and industry.

Investigate the expected protection requirements associated with the implementation of new systems, COTS products and diverse information distribution requirements. Evaluate latest DOD and industry measures to safeguard information.

Investigate methods to improve the ability of DOD to measure and test for readiness of information systems to provide IA.

Investigate viability, related issues and possible implementation methods to determine if Red Team testing and certification of DOD information systems could be outsourced to private industry.

Investigate and make recommendations on possible approaches for creating an organizational process that would provide guidance for outsourcing to industry.

Tasking documentation is contained in Appendix A.

1.4.1 Study Approach/Process/Procedures

The study began in May 1998 and was supported by individuals from the following companies and organizations: Booz • Allen Hamilton, General Dynamics, Georgia Tech Research Institute, C3I, Delfin Systems, ITT Industries, MITRE, Information Management Group, SAIC, GRC International, CSC, GTE, Harris and TRW. An official from DOD's IA Directorate provided liaison and support assistance. The study team organized by assigning a lead member plus other individuals to each of the above six terms of reference. The study team gathered data by various means including reviewing documents and publications, visiting DOD organizations and military commands and units, and holding discussions with key DOD civilians and military officers, as well as with senior industry officials.

1.5 DOD Actions And Activities

No one can argue with the fact that the DOD has taken the lead on IA within the government. It was bound to happen not only because of Congressional interest and pressure, but also because the military services have become so dependent on information systems. In the absence of direction from higher authority, the DOD decided to move out on IA in order to protect its people and systems. ***The catalyst for real action has been the influx of new action oriented civilian and military officials with a vision and a real sense of urgency***. They have made a difference. There is movement on all fronts. There is more IA awareness with policies and procedures being changed. New organizations have been established with their only functions being IA. Readiness, costs and risk management are being addressed. Red Teams have been active and vulnerability assessments are taking place. Tools and systems are being tested, Lessons learned and best practices are emerging. And there are more actions related to training and certification. Despite all of these activities, there are still some fundamental problems and a lot of room for improvement. These areas are discussed later in the report.

1.6 Telling It Like It Is

What emerged from the study team's efforts was a lot of facts with just as many issues and questions. Just as the explosion of information technologies has set in motion constant change, so has the efforts of the DOD. As mentioned above, there has been a flurry of activities related to IA. Not a week goes by without some type of action being taken by DOD agencies, offices and military units. For a variety of reasons, some aspect of IA is at the top of someone's action list. There are so many ongoing efforts it is almost impossible to keep track of what is occurring. Because of this, it quickly became clear that the entire set of this study's terms of reference could not possibly be addressed in depth in all cases. However, we have covered a lot of ground, gathered a good deal of information, and have a story to tell.

2. DISCUSSIONS

This section provides information on each of the Study's Terms of Reference (TOR). It also discusses other pertinent areas.

2.1 TOR - 1 Best Practices

This Study TOR asked the group to provide industry's view of best practices that can be employed to improve the level of IA across the wide range of DOD communications. Like many other areas of IA, today there are almost too many best practices to mention. As the IT world continues to move forward, best practices can change in days and months. However, in general terms, categories of best practices involve people, products, policies, procedures, processes, communications, management, responsibilities, risk, training, and assessment. Often best practices involve common sense which is frequently forgotten because of the hectic pace of everyday events. In industry, their own best practices always impact the bottom line - profitability. IT security/IA practices are often secondary to the need to make a profit. However, these factors increase a company's ability to make a profit. Very frequently, and if they apply to a specific product or service, companies are reluctant to make this type of information available to the general public. This is especially true when it involves information security which is considered to be very sensitive. Rather, it is reserved for their own internal use or their customers. In the DOD and other federal agencies IT security/IA practices are usually secondary to its mission to provide support to its customers. Although secondary, these factors should help improve the service provided to the customers. In some cases, we found that in both industry as well as in the government, best practices that make a difference are not promulgated to a large audience. In a few instances best practices involving vulnerability assessments were treated as if they were classified and closely held. To their credit, numerous DOD agencies, offices, and military units are implementing selected best practices. However, most are doing so only as it applies to its local environment. There is no DOD central management or focal point for best practices as they relate to IA. As a result, very often they are missing out on new or better best practices. Sometimes this can lead to serious problems. That is what occurred during when a specific company's software fix/best practice for one of their products did not get promulgated throughout the DOD to the system administrators who needed it as soon as possible (ASAP).

It should be noted that several other federal government agencies such as the General Accounting Office (GAO) and the General Services Administration (GSA) have established several best practices related to IT. One GSA example is a performance measurement guide called "Performance-Based Management: Eight Steps for Developing and Using IT Measures Effectively." The information in this guide is not new or unique. It is however, brought together in a concise manner which is easy to use and makes sense. In addition to government agencies and companies promulgating best practice, numerous other civilian and trade organizations are addressing specific areas such as software, networks, security systems, certification, training, incident response, computer security and tools.

The following best practices discussion addresses both general and specific areas. This information was compiled from numerous sources. All of these best practices are being used in varying degrees by some part of industry, DOD, other federal government agencies, and other civilian/commercial organizations.

The GAO studied the Best Practices of non-federal organizations recognized as having strong information security programs. These practices focus on the management framework because that is where it all begins. This effort recognized five major principles in which existed 16 best practices. The following is a summary of this information.

PRINCIPLES	PRACTICES
Assess Risk and Determine Needs	1. Recognize information resources as essential organizational assets 2. Develop practical risk assessment procedures that link security to business needs 3. Hold program and business managers accountable 4. Manage risk on a continuing basis

PRINCIPLES	PRACTICES
Establish A Central Management Focal Point	5. Designate a central group to carry out key activities 6. Provide the central group ready and independent access to senior executives 7. Designate dedicated funding and staff 8. Enhance staff professionalism and technical skills
Implement Appropriate Policies and Related Controls	9. Link policies to business risks 10. Distinguish between policies and guidelines 11. Support policies through central security group
Promote Awareness	12. Continually educate users and others on risks and related policies 13. Use attention-getting and user-friendly techniques
Monitor and Evaluate Policy and Control Effectiveness	14. Monitor factors that affect risk and indicate security effectiveness 15. Use results to direct future efforts and hold managers accountable 16. Be alert to new monitoring tools and techniques

A Summary of Sixteen Security Best Practices of Leading Non-Federal Organizations

Taking a cue from industry, the National Institute of Standards and Technology (NIST) has identified eight "Generally Accepted Principles and Practices for Securing Information Technology Systems." These eight principles provide an anchor on which the federal government should base its IT security programs including the area of IA. These principles are:

1. 1. ***Computer Security Supports the Mission of the Organization.*** The purpose of computer security is to protect an organization's valuable resources such as information, software, and hardware.

2. 2**.** ***Computer Security is an Integral Element of Sound Management***. Information and IT systems are often critical assets that support the mission of an organization. Protecting them can be as important as protecting other resources such as money, physical assets, and employees.

3. 3. ***Computer Security Should be Cost-Effective***. The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits.

4. 4. ***Systems Owners Have Security Responsibilities Outside Their Own Organizations***. If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be confident that the system is adequately secure.

5. 5. ***Computer Security Responsibilities and Accountability Should Be Made Explicit***. The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit.

6. 6**.** ***Computer Security Requires a Comprehensive and Integrated Approach***. Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This approach extends throughout the entire information life cycle.

7. 7. ***Computer Security Should Be Periodically Reassessed***. Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are

ever-changing. These and other issues make it necessary to periodically reassess the security of IT systems.

8. 8. ***Computer Security is Constrained by Societal Factors***. Various factors such as social issues may limit the ability of security to support the mission of an organization. For example, security and workplace privacy can conflict. Commonly, security is implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

Previously it was mentioned that the GSA had prepared a guide to help agencies develop and implement effective IT performance measures. This information was based on IT best practices from several sources including industry. The eight steps described in the guide are:

9. 1. ***Link IT projects to Agency Goals and Objectives***. The effective measurement of an IT investment's contribution to agency accomplishments begins during the planning stage. If done properly, IT investment planning is based upon the agency mission and strategic business plans.

10. 2. ***Develop Performance Measures.*** To assess the efficiency and effectiveness of projects, select a limited number of meaningful performance measures with a mix of short- and long-term goals. Measure the outcomes of the IT investment, not just its cost, timeliness and quality. An outcome is the resulting effect of the IT investment on an organization.

11. 3. ***Establish Baseline to Compare Future Performance***. Baselines enable agencies to determine whether performance improves or declines as a result of an IT investment.

12. 4. ***Select IT Projects with the Greatest Value***. In today's tight budget environment, agencies can only fund a limited number of IT projects. Value is based on the estimated economic return of an IT project/ investment plus its estimated contribution to an organization's business priorities.

13. 5. ***Collect Data***. The optimal time to focus on the data needed for the chosen indicators is during Steps 2 and 3 above. Agencies need to ask: "What data are needed to determine the output of the project? What data are needed to determine the effectiveness of the project?" Accuracy of the data is more important than precision.

14. 6. ***Analyze Results***. After obtaining results, conduct measurement reviews to determine if the project met the objectives and whether the indicators adequately measured results. A key question is "Do the results differ from what we expected?"

15. 7. ***Integrate with Management Process***. To assure that results improve performance, integrate them with existing management processes. If the results are not used, no one will take the measurement process seriously.

16. 8. ***Communicate Results***. Take the initiative to communicate results internally to improve coordination and increase the focus of workers and mangers. Communicate results with customers to foster and sustain partnerships.

The above high-level principles and best practices are being used successfully throughout industry and in some parts of the DOD and other federal government agencies. There are more detailed best practices which pertain to specific IT areas. All of these best practices are valid and should be used if possible by industry and government alike. For example, Carnegie Mellon's Software Engineering Institute and CERT (Computer Emergency Response Team) provide some 60 practices which describe the choices and issues that must be addressed to deal with network security. The Software Program Managers Network identified nine principal best practices observed to be used in industry, and deemed essential for nearly all DOD IT and other software development projects. The Department of Energy's Computer Incident Advisory Capability (CIAC) organization promulgated 16 Best Practices In Managing World Wide Web Server Security. The U.S. Senate asked a private company to build a best practice matrix for networks which describes performance indicators for "Minimum Essential", "Due Care", and "World-Class." Additional information and details on these and other best practices can be found in Appendix B.

2.2 TOR - 2 Tools

This Study TOR asked the group to gather statistics, analyze and catalog methods, procedures, processes and tools that have been used to support information security within DOD and industry. Early in the study it was agreed upon that the group would concentrate on the tools aspect of the TOR. DOD can not hope to make significant progress in information security and related areas without a significant set of tools to collect, maintain, analyze and present relevant data. This is another area where rapid progress is being made. The number of technology companies that deal with some aspect of IA continues to rapidly expand and now numbers in the hundreds. For example a security conference in July 1999 featured 300 companies showing thousands of security products and services. The same holds true for the number of related tools that are now available and it is almost impossible to keep track of them. Industry, educational institutions, "think tanks," not-for-profit companies and organizations, DOD (including the military services), and other federal government agencies are all trying to identify what is available, test and determine what works to satisfy specific needs, and promulgate this information to as wide an audience as possible. Tools fall into an expanding number of categories. In general terms they include those that " protect, detect, react and recover." The following is a more specific list of tool categories which cover most of areas related to information security:

Network Security Auditing (Scanning)
Network Intrusion Detection System (IDS)
Computer Security
Anti-Virus Software
Access Control
Anomaly Detection and Reaction (ADR)
Network Mapping
Vulnerability Scanner
Security Compliance Scanner
Web Filtering
Firewalls
Encryption
Content Checking
Source Authentication
Secure Protocols
Risk Analysis
Network Monitor
System Monitor
Infraction Scanner
Identification and Authentication

We believe that it would be very difficult to identify and catalog all of the tools that are being used to support information security within DOD and industry. We say this because there is no widely accepted focal point or authority for tools in either of these sectors. Absence this, many organizations are doing their own thing. Since there may be several different tools that address the same area, a given organization may use one, while a sister organization may use another. For example, this is the case within the military services. They do not coordinate their actions and, as a result, do not have a suite of common information security/information assurance tools. Another aspect of the tools question is whether or not they have been tested before they are widely accepted for use. The efforts in testing Commercial Off-The-Shelf (COTS) products described in the following Section (2.3) also applies to tools. In Appendix C we identify some of the tools that are being used today in government and industry. Information on methods, procedures and processes is contained in the Best Practices Section above and throughout the rest of this study.

2.3 TOR - 3 Commercial Off-The-Shelf (COTS) Products Use

This Study TOR asked the Group to investigate the expected protection requirements associated with the implementation of new systems, COTS products and diverse information distribution requirements, and to evaluate latest DOD and industry measures to safeguard information. Early in the study it was agreed upon to concentrate on COTS products. Global commercial technology forms the basis of information systems within the DOD and the government in general. For the DOD to carry out its mission, full and open cooperation with industry is required. Everyone recognizes that as technology continues to evolve at a rapid pace, there is an increase in the use of COTS products. This is taking place because COTS products are usually cheaper in price and easier to acquire. But these facts give rise to an IA concern that COTS is often associated with the "ease of access and interoperability paradigm" -- easier for us -- and for them. Threats continue to evolve just as technology does. In general, there is an absence of control and the future direction of COTS is uncertain. COTS products, hardware, and software move in directions determined by the commercial marketplace. In the DOD IA arena many officials are asking can we trust COTS? And if so, for what role? Should it be for non-mission critical use? Or in a developmental versus an operational role? Upon reflection it is clear that the DOD can neither afford to only develop organic systems nor can it afford to totally trust COTS. However, it is certain that the use of COTS products is here to stay. Given this fact, officials are searching for ways and means that can build necessary trust.

In today's Information Age, organizations are placing increased trust in the products, systems and technologies they use to create, process, transmit and store valuable information. This trust is a measure of the confidence or assurance that the product or entire system will perform reliably even in the face of unintentional or directed "attacks". One way to enhance trust is through testing. Formal testing has long been a prime method of assuring conformance to specifications. However, if a product or system is intended to provide security services, then confidence demands become greater and testing requirements become more complex and difficult. Trust in a product can be enhanced further when the product has been tested and certified by a competent, independent third party. Testing clearly adds value. But testing is not easy, and it's not cheap. Neither producers nor users will tolerate extensive costs or delays. Today there are few organizations able to perform competent, independent security testing, and even fewer effective methods for conducting security testing. However, it is essential that products must change to stay ahead of evolving threats; so must the tests, test methods, and metrics used to evaluate these products.

There are several ongoing government initiatives in this area. One is the National Information Assurance Partnership (NIAP), a collaboration of NIST and the National Security Agency (NSA). The goal of the NIAP is to help ensure the security of information technology systems and networks through cost-effective testing, evaluation, and certification programs. The NIAP is intended to foster the availability of objective measures and test methods for evaluating the quality of IT products. In addition, it is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services which will meet the demands of both producers and users. The International Common Criteria (CC) will be the focus of much of NIAP's work. The CC provides an internationally accepted criteria or standard for evaluating the security of IT products and systems.

Another initiative is NSA's Trusted Product Evaluation Program (TPEP). This effort evaluates security features and assurances of COTS products against the Trusted Computer System Evaluation Criteria (TCSEC) and its interpretations. The TCSEC associates defined levels of trust with ratings identified by digraphs (e.g. C2, B1, etc.). The results of the TPEP evaluations are published bi-annually in the Information Systems Security products and Services Catalogue Evaluated Products List (EPL) which provides a summary of an unbiased and authoritative evaluation of a product's suitability for use in processing classified and sensitive information.

The TPEP is actively involved in the establishment of commercial evaluation laboratories for the Trust Technology Assessment Program (TTAP) and the implementation of the CC. The TTAP is a joint NSA and NIST effort to commercialize the level of trust evaluation of COTS products. Under the auspices of the National Voluntary Laboratory Accreditation Program (NVLAP), TTAP is establishing, approving and overseeing commercial evaluation laboratories focusing on products with features and assurances characterized by the TCSEC. Companies desiring a level of trust evaluation will contract with an accredited laboratory and pay a fee for their product evaluation. TTAP approval and oversight mechanisms will assure continued quality and fairness using the NVLAP model of standardized testing and analysis procedures.

One other DOD effort is worthy of mention. The Defense Information Systems Agency (DISA) established the Joint Interoperability Test Command (JITC) at Fort Huachuca, Arizona. The JITC has recently developed new IA Test and Evaluation (T&E) laboratories which provide fee for service capabilities. Included in these capabilities is an ability to assess IA hardware, systems, networks, and processes. The JITC claims that this capability also covers the testing of COTS products.

The concern over the use of COTS products is now more widely known throughout the DOD and industry. Many initiatives by different organizations are underway or in place. However, as is the case in other areas, there is no central management, focus or direction. Dedicated people and organizations are doing their own thing often marching to a different drummer. Someone or some organization has to take charge. Results of all actions must be shared so that all authorities are aware of risks to their assets, systems, and missions. Last but not least is a requirement to have DOD and industry establish a partnership related to COTS products. This partnership should be full and open and built upon a foundation of mutual trust.

2.4 TOR - 4 Readiness

This Study TOR asked the group to investigate methods to improve the ability of DOD to measure and test for readiness of information systems to provide IA. One of the biggest questions that has to be answered is whether or not DOD agencies and military commanders will be willing to accept and trust contractors to provide IA support. Given that IA is a readiness criteria, how would outsourcing impact operational readiness? DOD units are measured by readiness standards and IA affects readiness. A non-trivial part of this issue is how IA readiness is defined. Make no mistake, this is an important but difficult subject. Defining IA readiness metrics is one of the biggest challenges facing both the DOD and industry. Why? Because there are none that are widely accepted. As with many other IA subjects, forward progress has been slow. This shouldn't have been the case since IA readiness concerns surfaced at least five years ago. The November 1996 Defense Science Board (DSB) report on Information Warfare (IW) Defense identified specifics regarding the need for process and recommended ways to incorporate IA readiness reporting in the current readiness reporting structure. (Appendix D provides excerpts from the DSB report). Since then other DOD organizations have tried to address this subject. The OASD/C3I tasked the Joint Chiefs of Staff (JCS) Information Assurance Division (J6K) to develop an IA reporting Policy. While progress has been slow to date because of fiscal and personnel shortages, there is renewed emphasis and activity.

All military units must report readiness status via two reporting systems. The Status of Resources and Training System (SORTS) provides a more straight forward bean-counting approach to readiness: % of personnel, % of equipment, % of supplies, etc. It does not provide measures for any IA readiness reporting. The Joint Monthly Readiness Report (JMRR) provides for a more subjective commander's report concerning the ability to execute specific scenarios. There are two parts to IA readiness reporting: developing a process and developing appropriate metrics. After discussions with the JCS staff and some combatant commands, the IA readiness process would involve using the familiar Protect, Defend, and React paradigm:

Identify missions and functions
Identify resources which support critical functions
Define needed IA capabilities (protect, detect, react/respond, and restore)
Establish reporting metrics
Define reporting process

The development of IA readiness metrics has evolved to the point where many officials are beginning to think that it will be modeled on existing readiness metrics as follows.

We currently assess Force Readiness on multiple levels:

At the individual unit level (ability of DIV, Ship, Wing to do their job)

At the joint force level (ability integrate and synchronized for missions)

At the aggregate or strategic level (ability of Combat Support Agencies (CSA) to meet national strategy)

Metrics for IA readiness should consider that criticisms of current Force Readiness centers around:

Inability to signal impending change

Imprecise ratings for unit readiness and training

Vague descriptions of readiness deficiencies and planned remedial actions

One part of the metrics approach would adapt the SORTS bean-counting methodology and the same parameters. This would probably be focused more on lower level commanders. For example:

SORTS Metric	Potential IA Metric
Personnel Indicators	**IA Readiness Personnel Indicators**
• Re-enlist • % of turn-over in near-term • % authorized personnel assigned	• % IA personnel re-enlist • % of IA personnel turn-over in near-term • % authorized IA personnel assigned
… and so forth	

This general approach could be extended to the other SORTS indicators such as Equipment Availability, Equipment Condition, and Training.

The other part of the IA readiness approach would be to model more on the JMRR approach to readiness and accept that mechanical bean-counting will probably not provide a completely satisfactory insight into current readiness. Therefore, a more subjective approach from higher level commanders could model on the Protect-Detect-React framework. One example could be something like:

PROTECT	**C-1**	**C-2**	**C-3**	**C-4**
“Defense-in-Depth” in securing systems and networks.				
Trusted operating systems and databases				
Access control				
Applications security				
Encryptors (KG/KY/FORTEZZA)				
Firewalls				
…and so forth				
PROTECT WAN	**C-1**	**C-2**	**C-3**	**C-4**
For classified networks, provide the strong, NSA-certified cryptographic privacy services capable of protecting national security information on a network wide basis/system high basis				
For all networks, protect the control layer to ensure network availability countering denial of service attacks.				
Encrypt networks for strong cryptographic protection of national security information (when applicable)				
Bulk encryption				
Sonet encryption				
In-line Network Encryptors (INEs)				
…and so forth				

That means adapting both the SORTS and JMRR methodologies and parameters to accommodate IA. While much more work needs to be done, it is reasonable to expect that industry will participate in the development and implementation of IA readiness processes and metrics, and continue to provide assistance in IA readiness supporting activities (exercises, Red Teams, vulnerability assessments, etc.). However, it is unlikely that industry will be allowed to actually measure IA readiness for military commands. It should be noted that there are no standards or widely accepted procedures for measuring IA readiness in industry. Rather, individual companies are or have been taking separate actions tailored to fit their specific needs. For example, the automotive industry has adopted a “just in time” parts inventory system wherein parts arrive at assembly plants just when they are needed. If parts are available, the plant operates; if any disruption occurs, the plant shuts down. Other companies have become virtual utilizing a world-wide communications network to fulfill product orders. If the system is not fully available, backlogs and distribution disruptions occur. As is the case in the DOD, these companies have also been moving at a slow pace because of a lack of dedicated resources and not fully utilizing IT resources.

2.5 TOR - 5 Red Team Training And Certification

This Study TOR asked the group to investigate the viability, related issues and possible implementation methods to determine if Red Team testing and certification of DOD information systems could be outsourced to private industry. Early in the study it was agreed upon that the group would also look at training and certification of people involved in Red Teaming as well as legal and contractual considerations. DOD’s definition of an IA Red Team is “an independent and threat-based effort by an interdisciplinary, simulated opposing force which, after proper safeguards are established, uses both active and passive capabilities on a formal, time-bounded tasking to expose and exploit IA vulnerabilities of friendly forces as a means to improve the readiness of DOD components.” How does industry fit into this definition from both operational and legal considerations since DOD is now using more and more contractors to support these activities?

DOD is moving forward at a rapid pace and numerous Red Team organizations have been established and Red Team activities are being conducted. However, consistent structure and approach to the problem, including taxonomy, terminology, methodology, process, metrics, and results reporting, have been lacking.

In May 1998, a draft of DOD’s Defense Information Assurance Red Team (D-IART) Methodology was promulgated by OASD/C3I. It specified a process for planning and conducting Red Team activities, and included metrics, a high level taxonomy of IA “attacks”, an analysis of skills and equipment required for attacks, and identification of available tools to assist in Red Team activities. The D-IART methodology was expanded from its focus on IA techniques to encompass full-spectrum information operations as defined in current DOD doctrine and it includes psychological operations, electronic warfare, deception, physical destruction, operational security, and computer network attack. D-IART methodology addresses:

- Identification of assessment requirements, metrics that quantify critical parameters, and expected results
- Definition of rules of engagement
- Scope of activity (benign vulnerability to invasive exploitation)
- Coordination of the D-IART with system and exercise managers
- Design of scenarios and development of associated scripts
- Use of modeling and simulation to augment assessment
- Development, collection, and use of a standard set of IW tools
- Formulation of a consistent and comprehensive reporting process
- Operational security during D-IART activities
- Controls over distribution of D-IART findings
- Identification of legal issues involved in D-IART activities
- Identification of staff selection criteria
- Formulation of, and coordination with, complementary Blue Teams

The D-IART is an excellent guideline for Red Team activities. After being in coordination for over a year, the D-IART has recently been officially promulgated.

This TOR asked if Red Team testing and certification of DOD information systems can be outsourced to private industry. The answer is yes. On many events and in many forums, industry is currently providing IA support to DOD the government does not have sufficient manning nor expertise to conduct all such activities with internal sources. Outsourcing may be the government's only way to sidestep the shortage of skilled workers. Industry, for its point, contains a large pool of experience and qualified IA experts. Industry's continued participation must include consideration of the following causes.

- Contractual limitations and constrains
- Legal liability and indemnification
- Long term commitment to justify investments in personnel, training and equipment
- Consent
- Continuity of effort

It is apparent that only the government can perform certain function these include high-level policy formulation, Red Team operations scripting, and the development of Red Team Rules of Engagement. All other Red Team functions can be outsourced to industry.

2.5.1 Training And Certification

An area of growing interest is IA training requirements throughout the DOD as well as in the private sector. This area involves awareness, certification and professionalization. DOD officials have stated that information superiority in the Department depends on a properly trained IA workforce. Because of the rapid advances in IT, training must be viewed as a continuum designed to maintain a knowledge and skill base that is highly perishable; it is not a one-time career event. A recent DOD Task Force identified the following vulnerabilities which have training as a common theme:

Lack of a common IA language, even among IA professionals

Lack of common training standards

Lack of assurance that DOD’s IA workforce, particularly those with privileged access, are held to some minimal training requirements before being given the “keys to the kingdom”

Lack of a consistent ability of the services and agencies to provide initial skill training to all members of the IA workforce, much less continuing training to maintain currency with the rapidly changing technology

Difficulty of maintaining currency of training curricula

Lack of common certification standards.

The level and content of IT/IA training in the DOD varies. In some areas there are comprehensive training programs available such as those for senior personnel at the National Defense University (NDU). In other cases, such as IA, training has been either unavailable or too expensive. As a result, the level of training for the IT/IA workforce has been uneven at best. However, the DOD is not sitting still in this area. It appears that all the services, NSA, DIA and DISA are attempting to provide a full range of IA training courses to their system and network administrators. Some of these courses are vendor- provided; some are computer based; some are mobile; and most are in a fixed location in a classroom. The Services and Agencies also provide IA training for Information System Security Managers (ISSM) and Information System Security Officers (ISSO). Only the Army and Air Force offers a formal training course for CERTs. DISA is developing a computer based CERT course targeting managers. No formal training is currently available for individuals on Red Teams or those who provide vulnerability or threat assessments. NSA has related vulnerability and threat assessment courses, but from an offensive, rather than defensive perspective. DISA is developing a hands-on exercise, using Computer Based Training (CBT), to teach system administrators and managers techniques to reduce threat and vulnerabilities to their information systems.

Several DOD organizations and senior officials have directed the services and other agencies to develop and implement certification plans for information system users, administrators and maintainers. Certification for classified networks is due in 1999 and for all other networks by the end of 2000. It is essential that any certification requirements be consistent, equivalent and transferable across all services and agencies. Further, formal certification should use common DOD standards. It is almost impossible to separate formal certification from training. There is a recognized process which involves various types of training followed by a period of observed performance and official designation of competency through documented certification. Because of rapid advances in IA technology, certification has a limited period of validity. As a result, re-certification is required to keep knowledge and skills current. A minimal certification process requires the following:

Evaluation, and periodic re-evaluation, of the categories of existing certification by existing experts to ensure that the categories of certification represent appropriate partitioning of the required expertise.

Examination, and periodic re-examination, of the certification requirements by existing experts to ensure that the requirements are complete, current, appropriate, and achievable.

Periodic examination of a sample of recently certified personnel by independent experts, to ensure that the certification process has sufficient rigor.

Collection of feedback from certified personnel regarding recommended changes to the certification process

A continuing education program, and re-certification process for certified personnel to reflect recent developments and changes in information technology

Collection and analysis of appropriate metrics on the certification process (e.g. % of pass/fail, etc.) to ensure that an appropriate, cost effective, and successful certification program remains in place

Because of the rapid changes in information technology, special attention must be placed on selecting the appropriate timeframes for all of the periodic activities listed above. It is recommended that the minimal acceptable period would be annual and the maximum would be two years.

The DOD has attempted to establish policy in this area through the promulgation of DOD Instruction 5200.40 entitled “DOD Information Technology Security Certification and Accreditation Process (DITSCAP).” This instruction implements policy, assigns responsibilities, and prescribes procedures for certification and accreditation of IT, including automated information systems, networks, and sites in the DOD. This is a fine document which contains a wealth of data. If implemented, followed and enforced, it will go a long way towards achieving its purpose. But this instruction concentrates on systems and not people. Further, this instruction does not attempt to define the management structure within the DOD, services or agencies that may be necessary to overall the certification and accreditation of DOD systems.

No one is able to accurately identify how much of the DOD’s IT/IA functions are being outsourced to industry. However, it is now becoming more known that contractors are performing many critical IA functions and the trend is expected to increase. Because of this, contractor personnel must be held to the same, or equivalent standards as government personnel. Contractual provisions are available for defining standards that must be met by contractor personnel. Certification requirements can be included as an attachment to the Statement of Work (SOW).

Because no common or widely accepted IA training and certification standards exist, the DOD and industry contractors are marching to a different drummer. As mentioned above, DOD services and agencies are devoting resources to IA training and certification. But this is almost an impossible task because the DOD is unable to determine precisely what IT/IA activities it is performing. The primary reason is that some people in non-IT/IA career fields are performing ill-defined IT/IA functions part time. This fact makes it difficult to determine who has access to DOD’s information infrastructures. Further, it is almost impossible to regulate training and certification requirements in what is basically a transient workforce. And finally, DOD training budgets vary to a great extent throughout the Department and it is very difficult to determine how much is devoted to IT/IA.

On the other hand, industry has a different view on training. Recent surveys have found that successful information technology companies show a total commitment to training investments. Those with the highest training expenditures measure them as a percentage of total payroll. Several companies spend over 15% of their payroll on training. Industry commitment to training is a basic instinct: it must have a properly trained, qualified, and in some cases certified, workforce in order to compete successfully for business. Furthermore, with the competition for IT professional so keen, industry uses training and certification as a big tool in trying to retain and recruit personnel (the military services also use this tactic). Industry is also leading the way in new and innovative approaches to training. CBT web-based training approaches, and distance learning are now becoming recognized as viable options. Commercial training institutions such as the Learning Tree provide almost instant access to various training tools and certification. Finally, simulation training such as wargames and interactive exercises offer portability, ease of use, and adaptability to ever-changing worldwide geopolitical and military environments. It is very difficult to determine how much DOD spends on total training, let alone how much is devoted to IT/IA. However, it is significant. It is known that the DOD spends 1% of its total budget on civilian training which equates to approximately $750 per person annually. As was the case before, it was also very difficult to determine how much of this amount was related to IT/IA.

2.5.2 Legal And Contractual Considerations

The legal issues are equal to, if not greater than, the management issues. They span the range of how IA support can be outsourced to industry to how to cover participants from liability exposure. Specifically, many issues must be addressed in order to ensure that outsourcing continues to be an asset which can be used. These include, but are not limited to:

Corporate and individual indemnification

Organizational conflicts of interest (COI)

Potential violation of 4th Amendment rights and Privacy Act

Use of non-disclosure agreements (NDA)

As part of the study, a panel was convened to address the above specific areas of concern. The panel was comprised of industry legal experts from companies (MITRE, CSC, TRW, BOOZ ALLEN & HAMILTON, GTE and GRCI) that currently provide, or have previously provided, some form of IA support. The panel concentrated on industry's participation in Red Team testing and certification of DOD information systems. A summary of discussions is provided in the following paragraphs.

Corporate Indemnification and Risk Management

What legal safeguards must be in place to protect companies involved in the red teaming of government-owned systems? When the government conducts Red Team exercises it assumes the risk of damaging its equipment and facilities, and of possible liability to its employees and third parties. By acting in the government's place in conducting such exercises, industry contractors would be exposed to the same range of liabilities. In principle, it is thus appropriate for the government to protect Red Team contractors from the consequences of such exposure to which they are subject only by virtue of acting in the government's stead. In so doing the government would not be undertaking any novel risk, and, as noted below, there are already existing proven mechanisms for accomplishing this necessary objective.

During the legal panel discussions, it became clear that government assistance would be necessary to adequately balance the performance risks inherent in Red teaming. In general, industry contractors will first look to insurance coverage to manage risks associated with performing these unique services. To the extent, however, that insurance is unavailable or is unduly expensive, the government should be required to shoulder some of the risk management burden and provide additional relief from third party claims and even prosecution where necessary. The following highlights some of the areas and mechanisms that might be employed to fill the risk management gap:

Loss or Damage to Government Furnished Property

Industry contractors are generally responsible for government property in their possession unless otherwise provided by the contract. In general, the industry contractor is not liable for loss or damage to government property provided under cost reimbursement or other types of contracts where the industry contractor has little direct control over the property (See Federal Acquisition Regulation (FAR) 45.103). This protection is not available, however, if the loss or damage to government property results from willful misconduct or lack of good faith on the part of the industry contractor. Thus the government and industry contractor would have to agree in advance that the provision of Red Team services that result in the destruction of government property will not constitute willful misconduct or lack of good faith. It may also be noted that the usual cost-reimbursement government property clause does not allow reimbursement for the cost of insurance (See FAR 52.245-4). If Red Team insurance is unduly expensive, relief from this restriction may be appropriate as well.

Indemnification under Research and Development (R&D) Contracts

Certain DOD R&D contracts may provide industry contractors with indemnification from claims made by third parties or even damage to a contractor's own property. The indemnification against a risk that is defined as "unusually hazardous" by the contract and arises out of the direct performance on the contract. Government indemnification here begins after the industry contractor's insurance is exhausted (See 10 U.S. Code (USC) 2354). To access this coverage, the government would have to agree that Red team contracts constitute R&D, and that the carefully defined scope of work for Red Team exercises was defined as "unusually hazardous" activity by the contract documents.

Public Law (P.L.) 85-804 - Unusually Hazardous Risks

Contracts that are not specifically for R&D have sometimes included government indemnification under P.L. 85-804. These clauses offer the contractor indemnification against a risk that is defined as “unusually hazardous” by the contract where the risk arises out of the direct performance on the contract. As noted above, the government’s indemnification responsibility begins after the contractor’s insurance coverage is exhausted. This type of relief has typically been offered in programs involving nuclear power or highly volatile rocket fuel. To access this coverage, it is likely that the government would have to formally expand the definition of “unusually hazardous” to include Red Team activity.

Careful Definition and Government Approval of the Statement of Work (SOW)

In each Red team exercise, the definition and government approval of the SOW would be necessary not only to conduct an effective exercise but also to define the activity for insurers and to classify contemplated activities as “unusually hazardous.” In particular, the government should approve reasonably precise specifications; the contractor should ensure that the Red team exercise is conducted in conformance with those specifications; and the contractor should provide the government with any and all information it possesses concerning the dangers associated with the conduct of the exercise, especially if these are not known by the government. Such precise approval of the proposed SOW may allow contractors to claim the protection of the government contractor defense against tort claims made by third parties.

Agreements Not to Prosecute

In the course of providing Red Team services, the contractor may technically violate some laws associated with the improper use of telecommunications resources, computer security, or other protected areas. The government should provide some level of immunity against prosecution for these violations.

Organizational Conflicts of Interest (COI)

Should industry contractors that support Red Team testing be restricted from participating in related procurement opportunities from the sponsoring government organization? The FAR 9.5 (Organizational and consultant COI) provides sufficient safeguards to protect the integrity of the procurement of Red team testing and remediation of system defects without unduly limiting the government’s flexibility in obtaining the necessary services. As such, contractors should not be restricted from participating in related procurement opportunities from government organizations targeted in the Red Team activity. The outsourcing of Red Team activities does not present ant insurmountable conflicts.

Regulations

OCI means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the government; or the person’s objectivity in performing the contract work is or might be otherwise impaired; or a person has an unfair competitive advantage (FAR 9.501).

The FAR identifies four main scenarios in which such conflicts generally occur: 1) providing systems engineering and technical direction (FAR 9.505-1); 2) preparing specifications or work statements (FAR 9.505-2); 3) providing evaluation of offers (FAR 9.505-3); and 4) obtaining access to proprietary information (FAR 9.505-4). Each of these scenarios is discussed with appropriate exceptions and safeguards identified based upon extensive procurement experience. The Contracting Officer (CO) is provided extensive guidance in handling these matters (FAR 9.504). The FAR (9.504) recognizes that potential organizational COIs may be avoided, neutralized or mitigated. Furthermore, the FAR (9.503) provides for a waiver of the OCI procedures if their "application in a particular situation would not be in the government's interest." A waiver must be approved by the agency head or his/her designee.

Red Team Testing

Many information technology contractors have broadly based capabilities to design and implement systems, including the security requirements of those systems. Such contractors can often provide both services. Others are specialized in one or the other area. Accordingly, a mitigation plan which establishes "firewalls" between such operations, which prohibits the unauthorized transfer of sensitive procurement information or contractor proprietary data, and which provides a mechanism for reporting any possible breaches should satisfy the government's requirements to avoid organizational COIs while performing Red Team testing.

In some instances, it may be desirable for the government to have the Red Team testing contractor both carry out the test and then provide an immediate fix for any critical weaknesses or flaws discovered. The contractor who finds the flaw may be uniquely qualified to fix it. Also, the time sensitive nature of fixing any discovered flaws may require the government to include this requirement in the SOW for the Red Team testing contractor. Testing may also reveal a flaw that only a limited number of contractors (perhaps only one) can fix. This may include the Red Team testing contractor that found the flaw. In these and other similar situations which may emerge, a mitigation plan may be appropriate. Alternatively, a waiver may clearly be in the government's best interest as contemplated by the FAR (9.503).

Designated Waiver Official

Since the issue of system security has such a high priority in government operations, requires very specific technical expertise, and is so highly visible in the event of failure, consideration should be given to making a special delegation of agency authority for the granting of waivers. Doing this in advance of beginning Red Team Testing, and notifying the COs of the responsible waiver official will speed processing if a waiver is required. Establishing a single point of contact will also assure that the regulatory principles will be consistently applied in the technical area of operations. The same designated official could also review the OCI mitigation plans for this technical area to assure that the government's interests are adequately protected.

Non-Disclosure Agreements, 4th Amendment Concerns and Privacy Act Issues

Non-Disclosure Agreements (NDAs)

NDAs should serve as an important safeguard for Red Team activities. The use of a NDA could be specifically delineated in the organizational COI clause of the contract between a government agency and a contractor and would serve as the basis for protecting the sensitive nature of the information viewed and generated by Red Team participants.

The NDAs would prohibit both the contractor and its employees from divulging any information obtained or generated during Red Team activities for any other purpose other than those called for by the contract without the consent of the cognizant government agency.

While a company-level NDA would conceivably provide the requisite protection, an additional level of commitment could be achieved by requiring the contractor’s employees themselves to execute an individual NDA as well. Not only would this emphasize the importance of non-disclosure principles to those individuals, but it could also serve as part of a firewall plan to allow Red Team contractors to engage in follow-on business with the cognizant government agency by segmenting its Red Team players from other parts of its operations.

4th Amendment Concerns

The constitutional protections of the 4th Amendment (freedom from unwarranted search and seizure by the government) would most likely not be impacted by Red Team activities.

The most likely scenario in which a 4th Amendment issue would arise is if Red Team activities uncovered illegal activity by a government employee involving the use of their government furnished computer. Theoretically, a government employee facing criminal punishment or agency discipline for wrongdoing could claim the government agency or the contractor violated his/her 4th Amendment rights by virtue of Red Team access into their computer or computer-related activities.

A solid defense against such a claim of a 4th Amendment violation is that the government employee does not have the legitimate expectation of privacy required by law with respect to government-furnished computer hardware and software. Strengthening this argument would be the fact that most government agencies have an explicit disclaimer for their personnel that puts them on notice that they are only to use the government’s computer systems for business purposes and that the agency reserves the right to monitor their usage.

An additional issue is whether or not a contractor would have a legal obligation to report evidence of certain criminal conduct to law enforcement authorities, independent of reporting to the government agency itself. Although it appears unlikely that any law would prohibit a Red Team contractor from first disclosing criminal wrongdoing to the government agency, there may be certain federal or state statutes that would place specific additional reporting obligations on the contractor. These would need to be examined on a statute-by-statute basis to determine what impact, if any, would have on Red Team activities.

Privacy Act Issues

The Privacy Act should not present any significant barriers to Red Team activities. This Act was put into place in 1974 and generally is designed to protect individuals with respect to the federal government’s ability to maintain and/or release information impacting on their personal privacy.

The Privacy Act compels federal agencies not to disclose personal information (i.e. social security numbers, employment records) without the written consent or under certain specific conditions. It also allows individuals to request access to the information maintained on them by a government agency.

So long as Red Team activities do not result in compiling new personal information on individuals, and sufficient protections, such as strong non-disclosure provisions, were in place to prevent Red Team participants from disclosing any personal information they came in contact with during their activities, the Privacy Act should not be impacted.

2.6 TOR 6 Organization

This Study TOR asked the group to investigate and make recommendations on possible approaches for creating an organizational process that would provide guidance for outsourcing to industry. Early in the study it was agreed upon that the group would concentrate on providing a draft of a Concept of Operations (CONOP) or Standard Operating Procedures (SOP) for Life Cycle Management of IA processes and procedures. This is an important area because there has been no IA standardization across the DOD. One organization may have a totally different understanding of IA than another. Current policies, procedures and processes are formulated by numerous DOD offices, agencies and military commands. Additionally, many such constructs are applicable only to one organization, agency , system or some other relatively small segment of the information infrastructure. Though high level policies and procedures do exist within DOD, numerous studies and reports have concluded that many decision makers are not even aware of their existence. Clearly some other model is required.

2.6.1 Information Assurance Center

Our study efforts concluded that some concept of a high level focal point or center would be a giant step forward. We are aware that the DOD already sponsors 13 Information Analysis Centers (IAC) and the Information Assurance Technology Analysis Center (IATAC). We do not propose duplicating the functions of these centers. Our idea (the center could have any number of names) is for DOD to have a “one stop shopping center” that would cover a wide range of IA activities including providing outsourcing guidance to industry. We looked at many examples and determined that the following general guidelines are pertinent for this organization:

Be established at a high level within the DOD. There should be subordinate “shadow” organizations within each military department.

Function as a “honest” broker” / “trusted agent” for all customer organizations

Be informative. It should collect and maintain a data / knowledge warehouse. This includes compiling statistics, analyzing trends and publishing this information.

Provide for training in IA concepts, policies, guidelines and operational procedures. Ensure that IA training materials are available and provided to users.

Ensure that a variety of IA awareness materials (e.g. posters, magazines, pamphlets, etc.) are designed and published on a regular basis.

Establish and control an IA certification process.

Provide guidance to include operational processes, procedures, checklists, etc.

Provide “pre-inspection survey” support to customers as needed/requested (i.e. help identify and rectify deficiencies before formal inspection process and before they become a problem).

Center would consist of a permanent core team of DOD civilian and military personnel. This would include procurement and legal personnel with experience in contracting with industry. As required, the center would be augmented with industry contractor support to provide a standing and readily available pool of subject matter experts.

Manage the outsourcing of IA functions to industry in accordance with (IAW) approved rules, regulations and procedures.

Identify problem areas and work with customers and other organizations to develop and implement corrective actions.

2.6.2 Outsourcing Guidance

This section focuses on the development of notional guidance that can be used within the DOD to direct IA outsourcing activities. For the purposes of this study, only those activities dealing with Red Teaming will be considered. In broad terms these activities include consideration of acquisition, operations, and oversight of the Red team process.

As part of our analysis, we evaluated Red Team processes to determine if these activities could be divided into guidance categories. In other words, if the Red Team processes can be finitely defined for analysis, then, using a set of decision criteria, the processes should naturally fall into three broad decision categories:

Always Outsource

Situational or “sometimes” outsource

Never Outsource

In this way, a rational and subjective evaluation of the processes can be made. The result of this analysis is a list of activities or processes sorted into the three decision categories. This list can then be incorporated into evolving IA policy documents. This list can also be used to develop a generic SOW for use by policy and acquisition personnel in obtaining services or as the basis of a solicitation to establish an omnibus contracting vehicle for procuring IA services.

The method used in our analysis attempt to apply a low-level scientific approach to the solution of a complex and multi-dimensional problem. The selection of methodologies involved a trade off between complexity of method, simplicity in dealing with a problem that has not been fully defined, and finally, the desire to create as objective a decision process as possible. We also hoped to reduce potential problems associated with any outsourcing decision by parsing activities and processes into defined decision categories.

As a starting point, five top level process areas were used: Policy, Vulnerability Assessment, IA Acquisition, Red Team Operations, and Certification and Accreditation. In order to gain a better understanding of the issues attendant to outsourcing, the development of guidance, and to ensure the greatest degree of objectivity, a number of process sub-areas were defined as follows:

Policy
Policy Decisions
Staff Support

Vulnerability Assessment
Technical Evaluation
Data Collection
Metrics Generation
Metrics Analysis
Report Generation

IA Acquisition
Program Management Support
Engineering and Technical Service
Life Cycle Logistics Support
Training
Contracting
Tools

Red Team Operations
Scheduling
Scripting
Oversight
Rules of Engagement (ROE)
Training
Data Collection
Analysis
Report Generation

Certification and Accreditation
Policy
Training
Certification
Accreditation
Data Collection

Before the outsourcing potential of activities could be evaluated, a set of evaluation criteria had to be established. We looked at criteria that would provide the most objective and most quantifiable assessment. The criteria selected included:

Cost/Cost Effectiveness

Long-term Capability

- Expertise
- Continuity

Flexibility

- Availability
- Expandability
- Tailorability

Accountability

Legal Issues

Political Sensitivity

Security

The expected results of an assessment would be a spread of scores for the selected outsourcing candidate activities with which to make a decision. Under ideal circumstances the IA activities would fit into tight groupings with little decision ambiguity. In this regard the most desirable outcome would be a clear set of scores that would easily discriminate between the principal outcomes of: Always Outsources” and “Never Outsource”. If ambiguity exists, the decision would require a case by case assessment. This area would include the results that fall between the extremes of Always Outsource and Never Outsource and would be characterized as “Situational or Sometimes Outsource”.

Having defined the IA activities to be assessed and the criteria to be used, input values had to be assigned to each of the activities relative to the various criteria. We used the following adjective input values:

H = Higher

L = Lower

S = Same/Equal/Equivalent

N = Not Available/Absence/Very Difficult

D = Difficult

E = Easy

V = Very Easy

Figures 1. and 2. depict the results of a hypothetical example of an assessment which involved relative comparisons between industry/contractor and military/government performance of an activity.

The resulting decision recommendations revealed that 14 out of 17 activities, or 82%, fell into areas that could be outsourced

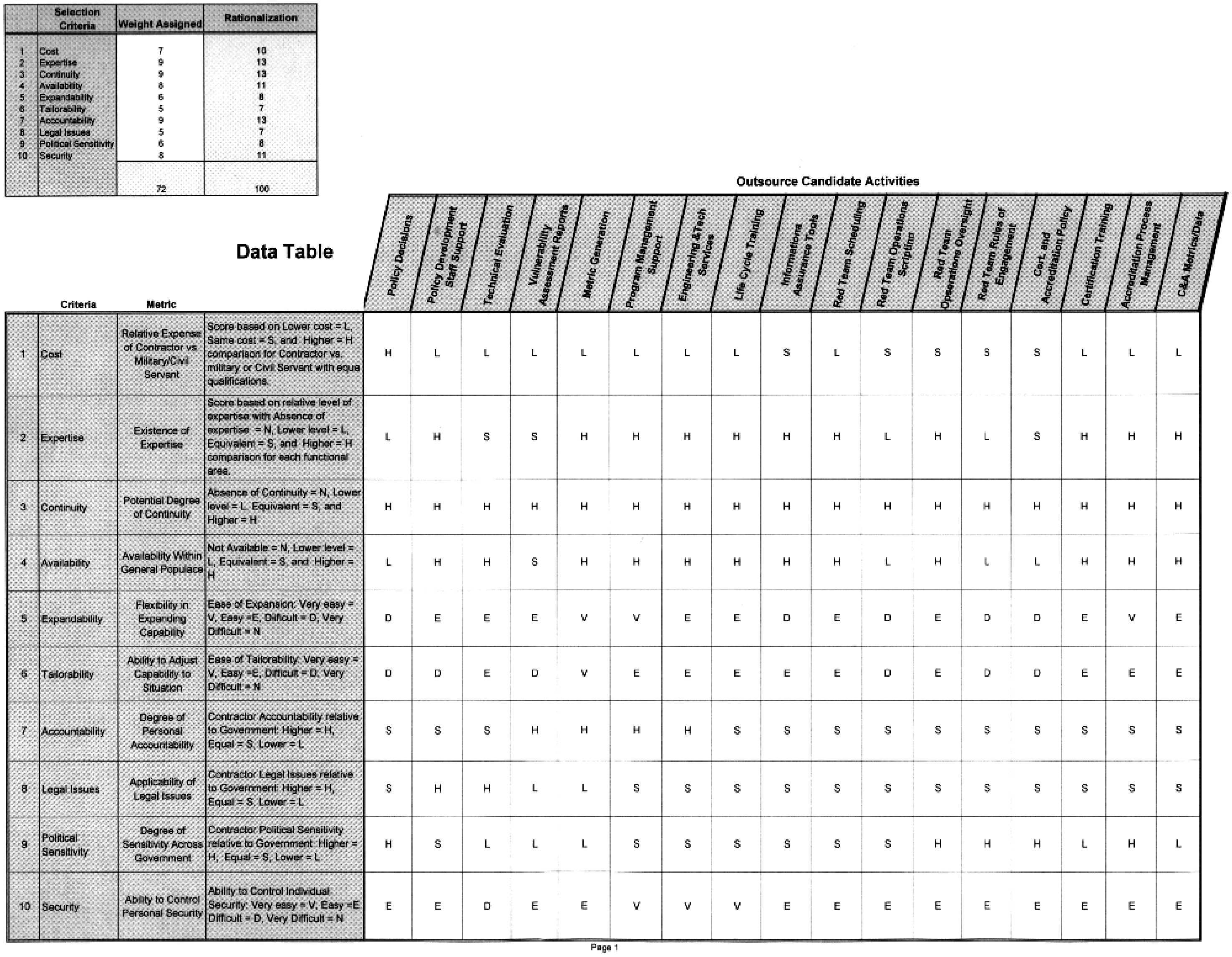
In evaluating the results of this analysis, it should be noted that a limited number of data points were calculated and a fairly coarse scoring scheme was employed. Inclusion of a wider range of activities with more levels of detail would enhance the value of this model. Additionally, if the scoring criteria were expanded to provide a wider range of adjective assessments, the scoring would tend to spread out across the range of scores from the highest to lowest possible. These refinements and expansion of the decision model would prove to be more beneficial and greatly enhance this important process.

2.6.3 Conclusions

The development of a set of high level policy guidelines for the potential outsourcing of IA activities to include the use of Red Teams is essential to the success of any undertakings. A useful by-product of this endeavor would be a concept of operations that contains the essence of the policy along with guidelines that are easily understood and can be used at any level of decision making. In each case, the decision-maker would have an easy to use desk reference to follow in the execution of IA outsourcing actions.

The analysis described above revealed that, under most circumstances, virtually every aspect of Red Teaming could be outsourced. As expected, the analysis confirmed that there are some activities of such a sensitive nature that they are not obvious choices for outsourcing and that they must be performed by government/military resources. These activities include high-level policy formulation, Red Team operations scripting, and the development of Red Team Rules of Engagement.

The actual distribution of decision recommendations from the above model lends itself well to the development of a generic Statement of Work (SOW) template for use in outsourcing. This template could easily be constructed and included in a DOD IA policy document in a section covering guidance for outsourcing. The template would contain information relative to those activities that could always be outsourced as well as those activities which fall into the situational



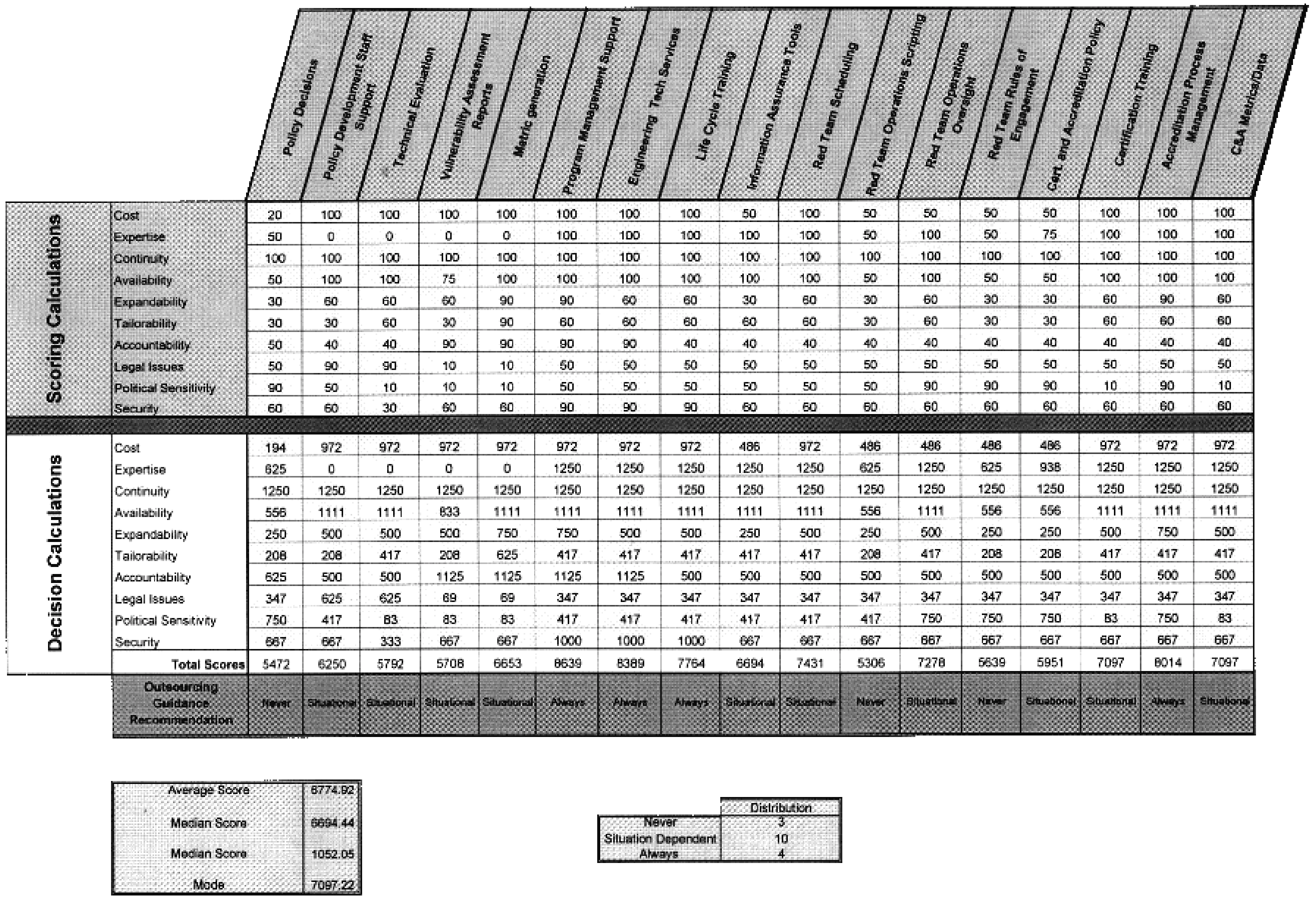
	Selection Criteria	Weight Assigned	Rationalization
1	Cost	7	10
2	Expertise	9	13
3	Continuity	9	13
4	Availability	8	11
5	Expandability	6	8
6	Tailorability	5	7
7	Accountability	9	13
8	Legal Issues	5	7
9	Political Sensitivity	6	8
10	Security	8	11
		72	100

Data Table

				Outsource Candidate Activities																
	Criteria	Metric		Policy Decisions	Policy Development Staff Support	Technical Evaluation	Vulnerability Assessment Reports	Metric Generation	Program Management Support	Engineering &Tech Services	Life Cycle Training	Informations Assurance Tools	Red Team Scheduling	Red Team Operations Scripting	Red Team Operations Oversight	Red Team Rules of Engagement	Cert. and Accreditation Policy	Certification Training	Accreditation Process Management	C&A Metrics/Data
1	Cost	Relative Expense of Contractor vs Military/Civil Servant	Score based on Lower cost = L, Same cost = S, and Higher = H comparison for Contractor vs. military or Civil Servant with equa qualifications.	H	L	L	L	L	L	L	L	S	L	S	S	S	S	L	L	L
2	Expertise	Existence of Expertise	Score based on relative level of expertise with Absence of expertise = N, Lower level = L, Equivalent = S, and Higher = H comparison for each functional area.	L	H	S	S	H	H	H	H	H	H	L	H	L	S	H	H	H
3	Continuity	Potential Degree of Continuity	Absence of Continuity = N, Lower level = L, Equivalent = S, and Higher = H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
4	Availability	Availability Within General Populace	Not Available = N, Lower level = L, Equivalent = S, and Higher = H	L	H	H	S	H	H	H	H	H	H	L	H	L	L	H	H	H
5	Expandability	Flexibility in Expanding Capability	Ease of Expansion: Very easy = V, Easy =E, Dificult = D, Very Difficult = N	D	E	E	E	V	V	E	E	D	E	D	E	D	D	E	V	E
6	Tailorability	Ability to Adjust Capability to Situation	Ease of Tailorability: Very easy = V, Easy =E, Dificult = D, Very Difficult = N	D	D	E	D	V	E	E	E	E	E	D	E	D	D	E	E	E
7	Accountability	Degree of Personal Accountability	Contractor Accountability relative to Government: Higher = H, Equal = S, Lower = L	S	S	S	H	H	H	H	S	S	S	S	S	S	S	S	S	S
8	Legal Issues	Applicability of Legal Issues	Contractor Legal Issues relative to Government: Higher = H, Equal = S, Lower = L	S	H	H	L	L	S	S	S	S	S	S	S	S	S	S	S	S
9	Political Sensitivity	Degree of Sensitivity Across Government	Contractor Political Sensitivity relative to Government: Higher = H, Equal = S, Lower = L	H	S	L	L	L	S	S	S	S	S	S	H	H	H	L	H	L
10	Security	Ability to Control Personal Security	Ability to Control Individual Security: Very easy = V, Easy =E Difficult = D, Very Difficult = N	E	E	D	E	E	V	V	V	E	E	E	E	E	E	E	E	E

Page 1

Figure 1. Red Team Outsourcing Assessment



		Policy Decisions	Policy Development Staff Support	Technical Evaluation	Vulnerability Assessment Reports	Metric generation	Program Management Support	Engineering Tech Services	Life Cycle Training	Information Assurance Tools	Red Team Scheduling	Red Team Operations Scripting	Red Team Operations Oversight	Red Team Rules of Engagement	Cert. and Accreditation Policy	Certification Training	Accreditation Process Management	C&A Metrics/Data
Scoring Calculations	Cost	20	100	100	100	100	100	100	100	50	100	50	50	50	50	100	100	100
	Expertise	50	0	0	0	0	100	100	100	100	100	50	100	50	75	100	100	100
	Continuity	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
	Availability	50	100	100	75	100	100	100	100	100	100	50	100	50	50	100	100	100
	Expandability	30	60	60	60	90	90	60	60	30	60	30	60	30	30	60	90	60
	Tailorability	30	30	60	30	90	60	60	60	60	60	30	60	30	30	60	60	60
	Accountability	50	40	40	90	90	90	90	40	40	40	40	40	40	40	40	40	40
	Legal Issues	50	90	90	10	10	50	50	50	50	50	50	50	50	50	50	50	50
	Political Sensitivity	90	50	10	10	10	50	50	50	50	50	50	90	90	90	10	90	10
	Security	60	60	30	60	60	90	90	90	60	60	60	60	60	60	60	60	60
Decision Calculations	Cost	194	972	972	972	972	972	972	972	486	972	486	486	486	486	972	972	972
	Expertise	625	0	0	0	0	1250	1250	1250	1250	1250	625	1250	625	938	1250	1250	1250
	Continuity	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250	1250
	Availability	556	1111	1111	833	1111	1111	1111	1111	1111	1111	556	1111	556	556	1111	1111	1111
	Expandability	250	500	500	500	750	750	500	500	250	500	250	500	250	250	500	750	500
	Tailorability	208	208	417	208	625	417	417	417	417	417	208	417	208	208	417	417	417
	Accountability	625	500	500	1125	1125	1125	1125	500	500	500	500	500	500	500	500	500	500
	Legal Issues	347	625	625	69	69	347	347	347	347	347	347	347	347	347	347	347	347
	Political Sensitivity	750	417	83	83	83	417	417	417	417	417	417	750	750	750	83	750	83
	Security	667	667	333	667	667	1000	1000	1000	667	667	667	667	667	667	667	667	667
	Total Scores	5472	6250	5792	5708	6653	8639	8389	7764	6694	7431	5306	7278	5639	5951	7097	8014	7097
	Outsourcing Guidance Recommendation	Never	Situational	Situational	Situational	Situational	Always	Always	Always	Situational	Situational	Never	Situational	Never	Situational	Situational	Always	Situational

Average Score	6774.92
Median Score	6694.44
Median Score	1052.05
Mode	7097.22

	Distribution
Never	3
Situation Dependent	10
Always	4

Figure 2. Red Team Outsourcing Assessment Decisions

or sometimes outsource category. Activities too sensitive to outsource would be omitted from the SOW template.

In a scenario where an OMNIBUS IA services contract exists, the development of such a SOW template for use across DOD would assist in streamlining acquisition of IA services and assure consistent application of guidance.

As a result of this analysis, the following actions are recommended:

Develop a Concept of Operations for outsourcing IA functions to include Red teaming.

Expand the outsourcing decision model described in this section in order to support a more robust and thorough assessment of IA and Red Team activities.

Consider the development of a draft SOW for inclusion in any DOD IA outsourcing policy.

As part of this study we have drafted a recommended “Red Team Evaluation and Acceptance Criteria” which is contained in Appendix E and a recommended “Red Team Life Cycle Management” which is contained in Appendix F.

2.7 Other Pertinent Areas

2.7.1 Policy And Architecture

From available historical data, we estimate that this is approximately the seventy sixth (76) study which has addressed some aspect of DOD IA during the last three years. Sponsoring organizations have ranged from the Defense Science Board (DSB) to the Center for Strategic and International Studies (CSIS) with DOD internal office, military units, think tanks, and industry in between. Volumes of data has been gathered. The single common concern in all of these studies relates to policy and architecture. Today there is no commonly accepted DOD policy or architecture which covers all aspects of IT and IA. Not that there haven’t been attempts and we commend DOD’s continuing efforts. And as actions continue in this area, we believe that such a policy and architecture will become a reality. In the absence of guiding policy and architecture, individual agencies, offices, services and units continue to move forward taking individual IA actions. Because there is no accepted policy, officials can’t say that these actions are wrong. With regard to this study, we could not find any evidence of a policy and architecture which governs the outsourcing of IA functions to private industry. We believe that the development of such a policy or architecture is important and could be more easily achieved than the development of an overall IA policy and architecture. As DOD IA activities continue to accelerate and DOD resources continue to decline or be shifted, there will be a requirement to increase industry IA support provided to the DOD. In the not too distant future, we see a DOD agency telling another DOD organization that they should turn to company X for IA services because it cannot fulfill their IA request at that time. This of course means that the DOD has certified company X to perform those IA services. This is but one example of the details that would have to be addressed in developing an IA outsourcing policy and architecture.

We applaud DOD efforts began in 1999 to integrate and consolidate Pentagon and Office of the Secretary of Defense (OSD) Information Technology. This is definitely a step in the right direction.

2.7.2 Costs

In today’s fiscally constrained environment, cost is clearly a strategic factor. As is the case in industry, measuring cost is a critical capability for the DOD in order to understand return on investment and true long term cost factors. Everyone agrees that there has been a significant increase in overall DOD spending on IA. As a result, many officials proclaim that there have been significant improvements. And while specific examples can be identified, there is no accepted measurement to determine if the results were worth the cost. A number of senior officials and organizations contacted during the course of this study stated that this is one of the greatest challenges they face in IA. A number were concerned about who pays for IA assessments or Red Team costs? Who determines what information or networks should have maximum protection? In the absence of a measurement tool, individual decisions on return on cost investment are being made everyday at all levels. If more and more IA functions are going to be outsourced to industry, then the cost of doing this has to be taken into consideration. In addition to the concerns mentioned above, the DOD will have to pay to constantly certify the credibility of contractors to provide competent IA support. In order to be able to provide this support, contractors will have to maintain a cadre of qualified, trained, certified, and security cleared people at all times. To attract and retain these specialized technical individuals has a cost factor. Additionally, the cost of obtaining and maintaining clearances is not trivial. What to do with these people when they are not performing DOD IA support functions has certain cost implications. As the

DOD and industry gain more experience in the total IA arena, measuring returns on cost investment will remain a high priority concern. The DOD and industry should work together now to take advantage of work that has already been done and identify those tools and procedures which will automate and simplify this evaluation. The sooner that this takes place, the better.

2.7.3 Risk Management

Risk management is required in an environment when threats to information systems can come from numerous sources against a variety of targets both within the government and externally. Because 100% protection of information is not possible all of the time, risk management rather than risk avoidance is necessary. Risk management addresses the enduring question of " how much security/assurance is enough?" A key task in getting the answer is evaluating current assurance status/posture (i.e. measuring information assurance readiness). This is achieved with varying success, depending on how a given method assesses and aggregates effectiveness of safeguards against the consequences of successful exploitation of weaknesses by a threat action or event. Some risk management tools are qualitative and subjective, while others require quantitative inputs, such as numerical percent of safeguard effectiveness and dollar value of potential losses. Effective risk management must support the DOD agency or military unit by orienting on what is important - mission and operations - as outlined in the following process model:

Identify and Value Mission Functions and Enabling Information Resources. Identify and prioritize critical missions and functions and the information resources required to carry out these missions and functions. Assign value to systems and components under consideration. Orient on adverse operational effects from the loss of systems and components. Consider changes in the situation that relate to time, operational phases, etc. Prioritize systems and components based on these values.

Identify Threat. Identify and describe threat sources and agents and threat actions/events/situations.

Identify Vulnerabilities. Identify and describe system and component weaknesses and vulnerabilities (weaknesses exploitable by threat source/agent/action/event/situation).

Assign Value to Adverse Effects (Estimate Risks). Identify, describe and assign value to the consequences and impacts (nature, likelihood) of threat action/event situation against system and component vulnerabilities.

Identify and Select Safeguards/Countermeasures**.** Identify, describe and assign value to the potential safeguards/countermeasures against vulnerabilities. Assign value in terms of effects on threat and system and component and in terms of resources expended or their "costs" recommend and select safeguards/countermeasures based on clear decision rules.

Identify Residual Risk. Identify and assign value to residual risks that are "acceptable" (i.e. not dealt with or eliminated by safeguards/countermeasures.

Implement. Establish and operate safeguards/countermeasures. Continually monitor all factors and re-enter the process at the appropriate time.

Outsourcing IA Support to Industry and Implications for Risk Management.

IA support is currently being outsourced to industry and, from all indications, it will continue to increase in the foreseeable future. Because of this, one must ask how much of IA risk management functions will be performed by industry. The feasibility of conducting risk management on an outsourcing basis is influenced by important constraints and factors generated by the nature of the process and by the organizational environment.

First, the input requirements to perform a comprehensive analysis for any but the most simple of systems and networks are rather extensive and numerous. To ensure thorough coverage, the risk analysis must start with a solid understanding of the missions, supporting functions and operations, and enabling information systems.

Second, there must be sufficiently detailed knowledge of all relevant resources (computers, communication devices, peripheral equipment, telecommunications connections, personnel, facilities, procedures, etc.).

Third, risk management is an ongoing process that calls for sustained close attention to changes to any inputs. Oversight and monitoring must be of a sufficient duration and granularity.

Fourth, the magnitude and nature of the changes will demand a corresponding re-entry to the process with another iteration of analysis and decision- making. This calls for a fairly quick ability to act in response to these changes.

Fifth, conducting a risk management analysis by manual methods is no longer feasible because of the labor and time involved. This means that automated tools and the expertise to skillfully use them must be available.

Sixth, information systems are proliferating geographically and organizationally with almost bewildering complexity and at an explosive rate. Assigned technical personnel are already heavily burdened with responsibilities for planning, acquiring, installing operating and maintaining systems. Can these personnel keep up with this rapid pace of technology advancement on all fronts in order to do their everyday jobs? Can these same personnel also be expected to responsible for risk management functions? There may well be a requirement for additional personnel.

Seventh, agency and command personnel may be too close to a given situation to fully develop a valid assessment. An outside view might be able to make discoveries and generate insights that inside personnel might overlook. Also an industry team could bring expertise and lessons learned from being involved in situations while supporting other organizations.

Eighth, fact-finding and assessment visits by senior and/or external organizations are often viewed with some suspicion and anxiety. Foe example, the positive and negative impacts of an “annual general inspection” are well known in the military. Risk management teams operating in this mode, descending on an organization would probably encounter something less than the most conducive environment. Perhaps a trusted third party/honest broker could provide very productive risk management analysis and advice in a positive atmosphere.

One-time, ad hoc, short-term, perceived -as-threatening risk management studies conducted by higher echelons are not likely to satisfy all, or even most of, the requirements outlined above. Most especially, they would be less likely to provide the needed understanding of mission and operational needs and extensive, detailed and sufficiently sustained knowledge and trust.

The aggregate of risk management constraints and situational factors, in combination with the possible courses of action, suggest that risk management efforts might best be addressed with an outsourcing solution that has the following attributes:

Expertise in information systems operations, risk management procedures, and appropriate analytical and decision support tools

Trust, third party and honest broker

Sufficient dwell-time onsite to enable the wide-ranging detailed knowledge base and recognition of system changes

Furthermore, it is expected that limits on expanding DOD agency and military staffing will continue. Taking all of this into consideration, we believe that capabilities from the private sector could be assembled to meet this need. Industry would also have a measurably greater flexibility to acquire, train and retain expert personnel to keep pace with rapidly changing technologies.

3. CONCLUSIONS AND RECOMMENDATIONS

This section provides conclusions and recommendations as a result of the study.

3.1 Conclusions

3.1.1 The Answer Is

The Study Team was asked to determine if DOD IA support can be augmented through outsourcing to private industry. It quickly became apparent that ***the answer is a resounding yes!*** On many fronts and in many forums, industry is currently providing IA support to the DOD.

3.1.2 There Is A Market For IA Services

There is a market for industry support to government IA activities including Red Teams. The government does not have sufficient manning nor expertise to conduct all such activities with internal resources. Industry, for its part, contains a large pool of experienced and qualified IA experts who could be used to augment government assets. Industry wants to participate and looks forward to the opportunities and challenges that such efforts hold. However, the effort must make sense from a business perspective.

3.1.3 Industry Will Participate

Industry is interested in providing IA services to the government provided that certain issues are addressed adequately. These include but are not limited to:

Contractual limitations and constraints
Legal liability and indemnification
Long term commitment to justify investments in personnel, training and equipment
Consent
Continuity of effort

3.1.4 Red Team Activity Can Be Outsourced

While the government certainly needs to maintain control at every level as well as establishing policy, guidance and control functions, nearly all Red Team activity can be outsourced to industry.

3.1.5 Government Needs Industry Support

Industry support of and participation in IA activities is essential if the government hopes to be successful. There are simply insufficient internal government assets (both in breadth and depth) to adequately perform all required IA activities in any reasonably aggressive program.

3.1.6 Policy And Architecture Are Lacking

There is no commonly accepted DOD policy and architecture which covers all aspects of IT/IA. While there continues to be active attempts to fully establish such a policy and architecture, the goal hasn't yet been achieved. In the absence of a guiding policy and architecture, individual agencies, offices and military units continue to move forward taking individual actions to deal with IT/IA. Often there is duplication of efforts and it difficult to measure effectiveness in many areas. This lack of a policy and architecture is particularly apparent when it comes to dealing with industry participation in IT/IA activities. We could not find any evidence of any high level policy or architecture which governs outsourcing IA support to industry.

3.1.7 DOD IT/IA Organization Is Lacking

DOD is not properly organized to deal with the most important aspects of IT/IA/IO. There is no focal point with proper authority which can ensure commonality, synergy, standardization, responsiveness, awareness, training, staffing, testing, certification and budgeting across all of DOD to include the military services. We could not identify any single organization which has responsibility for dealing with outsourcing IA support to industry.

3.1.8 Costs Must Be Measured And Managed

Cost have to be managed by both government and industry. An acceptable way to measure return on investment must be established and agreed upon by all participants. The government needs to be fully aware of what services they are buying and industry has to be able to show that IA activity is a worthwhile business. Within the government, return on investment (ROI) needs to be calculated with more than accounting practices in mind. The observed practices of accounting for work done by government employees as “free goods” can lead to financially flawed decisions. ROI is a potentially useful tool for government agencies but appears to be essentially incompletely implemented.

3.1.9 There Are Legal, Liability, And Contractual Considerations

Legal issues are equal to, if not greater than, the management issues. Many issues must be addressed in order to ensure that outsourcing continues to be an asset which can be used. Current laws in the areas of computers, software, networking, information privacy and the liability issues associated with each, are only just beginning to be tested. It is almost certain that reevaluation of existing laws will be required as issues related to IA activities arise. We do not believe that the DOD has put enough emphasis on legal issues related to outsourcing IA functions. As a result, both government and industry organizations, as well as individuals involved in carrying out certain IA responsibilities, are being exposed to legal risks which could pose significant problems.

3.1.10 Risks Must Be Managed

Some level of risk is unavoidable. Considering the technology available today, it is unlikely that a completely “bullet proof” system could be built and even if it could, the cost would be prohibitive. Therefore risk must be evaluated, assessed, and managed within the constraints of operational readiness and budget allocations.

3.1.11 Information Flow Is A Concern

Information does not appear to flow well throughout the DOD. Many agencies and organizations do not always receive important information related to directives, required corrective actions, best practices, test results, industry alerts, etc. One example previously mentioned was that many DOD system administrators were not aware of a new commercial software upgrade which corrected a serious security problem. Another example was that many key senior ASD/C3I officials were not aware of this Study despite a Letter of Introduction from the Senior ASD/C3I Civilian who directs that office.

3.1.12 Inventory Of IT/IA Activities

For available information, it appears that the DOD is not fully aware of what IT/IA activities are being performed and by whom across its entire organization. Although there are many reasons for this, the primary cause is that both civilian and military personnel in non-IT/IA career fields are performing ill-defined IT/IA functions part-time. This is particularly significant because it makes it very difficult to determine who has access to DOD’s information infrastructures. It also appears that the DOD is unable to identify the number of industry/contractor personnel currently being used to carry out/support IT/IA functions.

3.1.13 Common IT/IA Language/Terminology

In several areas, the DOD has attempted to develop definitions that accurately reflect today’s IT/IA activities. While this is a good start, it must go further and address all IT/IA activities in all areas. This standardization would go a long way to preventing one organization of having a totally different understanding of a term from another organization.

3.1.14 Red Team Training And Certification

Red Teams are being used more frequently across all of the DOD and it appears that this usage will continue to increase. Their successes have varied depending on any number of reasons from access to people, processes and data, to acceptance by authorities, to capabilities/experience of team members. Industry has participated in these Red Teams and this support will also continue to increase. It is imperative that all people involved (government and industry) are properly trained and certified. Common training and certification standards should be established to include minimum and maximum timeframes to accommodate rapid changes in technology.

3.1.15 Readiness

IA is now accepted as a readiness criteria. However, there are still several “loose ends” that the DOD has to address. First and foremost is a widely accepted definition of IA readiness. Next is how to measure and test for the readiness of information systems to provide IA. And lastly is how to report IA readiness. There are several DOD organizations working on this subject. However progress continues to be slow. In the meantime other DOD organizations, particularly the military services are adopting their own ways and means to deal with this issue. We believe that the DOD has to quickly define what constitutes IA readiness and standardize readiness measurement metrics and IA readiness reporting.

3.1.16 COTS

IT/IA COTS products are becoming more numerous and cheaper. The use of these products by the DOD will continue to increase. This usage causes concern and officials are asking to what extent can they trust COTS products. We found that there are many initiatives underway in the DOD to test and evaluate these products. While we applaud these efforts, we found that there is no DOD central management, focus or direction. Dedicated people and organization are doing their own thing, often marching to a different drummer. We believe that direction, focus and management has to be implemented ASAP. Results of all actions must be shared so that all concerned are aware of risks. Also, DOD and industry should establish an open and trusting partnership to deal with COTS products.

3.1.17 Best Practices And Tools

Great amounts of information related to IT/IA best practices and tools is available from many sources. The numbers taken together are in the hundreds. Both the DOD and industry could learn a lot from this information. The major problem is how to assemble, keep track and make available all of this data. We could find no DOD organization which has this responsibility. As a result, each agency, office or military unit is left to their own discretion. This lack of synergy hampers efficiency, results in duplication, and can increase risks and vulnerabilities. Someone or some organization should take charge.

3.2 Recommendations

3.2.1 Policy And Architecture Must Be Established

DOD gives every indication that IT/IA is a top priority. The Study Team agrees with this philosophy. If this is the case, then DOD must continue its efforts to establish a definitive IT/IA policy and architecture which identifies roles, responsibilities, accountability, reporting responsibilities, etc. This policy and architecture should be established at a high DOD level and be acceptable to all DOD civilian and military organizations. If the development of this overall policy and architecture continues to lag, then we strongly recommend that DOD develop a policy and architecture which contains provisions that will allow the government and industry to continue to participate in IT/IA activities. This should include the outsourcing of IA functions to industry. We also recommend that the DOD continue its efforts in integrate and consolidate Pentagon and OSD IT.

We believe that DOD must move toward a longer range view and get away from short-term and quick-fix scenarios that it finds itself dealing with on many occasions. A well thought-out architecture with a realistic, funded, and high priority plan of action and milestones (POA&M) is highly desired.

3.2.2 Organizational Concept

DOD should adopt an organizational concept similar to the Information Assurance Center (IAC) previously described in Section 2.6.1. The best opportunity for success most probably takes the form of a brand new, high level, totally independent, IA specific organization with direct access to the Secretary of Defense and with authority for direct liaison with all external federal government departments, agencies and organizations. We view this organization to be a “focal point”/ “clearing house”/ “one-stop shopping center”/”data warehouse” for IA activities. Some existing IA related organizations should report to this new entity or be absorbed by it.

We agree with a DOD official who recently recommended the following: that the DOD appoint an IO integrator for all of the military services to ensure that synergy is achieved, redundant parallel efforts are eliminated, and suboptimization is detected: otherwise efficiencies will not be realized, and “risks accepted by one, will be shared by all.” We believe that the organizational concept we are recommending could assume this and other similar types of responsibilities for all of DOD.

3.2.3 Legal, Liability And Contractual Considerations

Section 2.5.2 of this study contains an extensive discussion of legal issues ranging from how IA support can be outsourced to industry to how to cover participants from liability exposure. The following recommendations are as a result of that specific effort:

When conducting IA and Red Team Activities, the DOD assumes the risk of damaging its equipment and facilities, and possible liability to its employees and third parties. The DOD should provide the appropriate levels of liability protection to contractors by virtue of acting in the government stead.

In support of IA and Red Team activities, contractors may technically violate some laws associated with the improper use of telecommunication resources, computer security, or other protected areas. The government should provide some level of immunity against prosecution for these violations.

IA and Red Team outsourcing requires careful definition and government approval of the Statement of Work(SOW). A well written SOW helps to define the activity for insurers and may allow contractors to claim the protection of the government contractor defense against tort claims made by third parties.

Non-Disclosure Agreements(NDA) should be strictly enforced to prohibit the release of any information obtained or generated during IA and Red Team activities. Further, the government should require the contractor to have each employee supporting IA and Red Team activities, execute an individual NDA to provide an additional level of confidentiality.

The SOW should have a clearly defined set of procedures for the reporting of illegal activities. These procedures should provide the contractor with guidance for additional reporting obligations (e.g. law enforcement authorities).

3.2.4 Best Practices

Both the DOD and industry can learn a lot from each other's best practices. (Best practices cover a wide range of activities including methods, procedures, processes, etc.) There is an incredible amount of information available that can greatly enhance overall IA operations and efficiencies. The problem is how to gather and keep track of all of this data. We recommend that the DOD task one of its organizations or support contractors with this responsibility. (If the IAC organizational concept described above is adopted, then that organization should carry out this task.) Taking inventory of best practices within the DOD and the rest of the federal government should be the top priority. A great deal of this information is readily available at various organizations' web sites. Identifying industry's best practices should come next. If industry resists, then DOD should first work with its current contractors and insist that they share their best practices within the scope of their existing contracts. The DOD should establish procedures to protect those industry best practices which have an economic advantages with regard to one company versus another. The compilation of best practices from government and industry will do no good unless it gets to the appropriate people and organizations in a timely manner.

3.2.5 Tools

What was recommended for best practices in Section 3.2.4 above pertains to tools as well. DOD must get a handle in this area because of the rapid proliferation of tools related in IT/IA and information security. There are literally hundreds of tools available and a lot of them are being used throughout DOD without any central management or focus. The following are but two examples which emphasize this point: one recent DOD IA publication identified 44 anti-virus tools; and the Navy's Information Security (INFOSEC) Web Site provides lists of tools, products and vendors that number over 200. Without a DOD focal point, valuable information on the latest in technology developments, usage experience and lessons learned can be lost or not made available to those who need it the most.

3.2.6 Commercial Off-The-Shelf (COTS) Products

The use of COTS products for DOD's IA activities is here to stay. The concern over the security of these products is now more widely known throughout DOD and industry. We commend the many initiatives related to testing and security enhancements now underway or in place. However, as is the case in other areas, there is no central management, focus or direction for these efforts. We recommend that DOD assign this responsibility to one of its organizations. Results of all actions must be shared so that all authorities are made aware of risks to their assets, systems, and missions and what mitigation is available.

3.2.7 Readiness

DOD has a real challenge on its hands as it attempts to find the ways and means to measure and test for readiness of information systems to provide IA. While much work has been done in this area, we could not find a widely accepted definition of IA readiness. Nor could we find that readiness measurement metrics have been standardized throughout the DOD. As a result, it is very difficult to measure DOD IA readiness. This in turn questions the ability of DOD units to deter anyone from exploiting vulnerabilities. We recommend that DOD continue its efforts to define IA readiness, standardize readiness measurement metrics, and IA readiness reporting. To ensure success, we also recommend that DOD devote adequate fiscal and personnel resources to these efforts.

3.2.8 Red Team Training And Certification

DOD is using Red Teams more and more to identify IA vulnerabilities, and to test and improve the readiness of its components. The DOD has established guidance and promulgated methodologies for Red Teaming activities. We recommend that this guidance and methodologies become standard practice and are strictly enforced.

DOD officials have stated that information superiority depends on a properly trained workforce. However, DOD has also declared that IA training and certification is a serious problem area with many vulnerabilities. We recommend that the DOD:

- Establish and promulgate common IA training standards
- Establish minimum training requirements for key IA personnel such as System Administrators and others before they assume their responsibilities
- Establish a process to provide initial skill training to all members of the IA workforce
- Establish a program for continuing IA training to maintain currency with changing technology
- Establish and promulgate common IA certification standards and a process to achieve certification for both government and industry personnel.
- Ensure that adequate fiscal and personnel resources are devoted to IA training and certification.

3.2.9 Costs

DOD is devoting a significant amount of resources to IA. As a result, a number of involved officials have proclaimed that there have been significant improvements. And while specific examples can be identified, there is no accepted measurement to determine if the results were worth the cost. As IA activities continue to expand, and as industry participation continues to increase, measuring returns on cost investment will continue to be a high priority concern. We recommend that DOD and industry join forces to take advantage of work that has already been done and identify those tools and procedures which will automate and simplify the evaluation of return on cost investment.

3.2.10 Risk Management

Because 100% protection of information is not possible all of the time, risk management rather than risk avoidance is necessary. Risk management addresses the enduring question of “how much security/assurance is enough?” A key task in getting the answer is evaluating current assurance status/posture (i.e. measuring IA readiness). Effective risk management must support DOD agencies and military units by orienting on what is important - mission and operations. We recommend that DOD develop and acquire risk management tools and utilize a risk management process (similar to the model described in Section 2.7.3).

It appears that IA support will continue to be outsourced to industry. The feasibility of conducting risk management on an outsourcing basis will be influenced by important constraints and factors generated by the nature of the process and by the organization’s environment. We believe that industry can perform certain risk management functions. We recommend that DOD use a risk management process to identify and select those areas where industry can provide this type of support.

3.2.11 Information Flow

Ensuring that the right people get the right IA information in a timely manner is a big challenge. Government and industry personnel must be more aware of vulnerabilities and their implications. DOD has faced similar information challenges in the past and designed methods to solve these problems. We recommend that DOD foster better communications through as many means as possible having a focal point assigned this responsibility would greatly enhance this effort.

3.2.12 Miscellaneous Recommendations

3.2.12.1 Common IT/IA Language/Terminology

DOD should develop and promulgate a common and acceptable IT/IA language and terminology

3.2.12.2 Inventory IT/IA Activities

DOD should determine precisely what IT/IA activities are being performed and by whom government civilian and military, and industry throughout its entire organization. Until this is accomplished, an IT/IA baseline is not possible.

APPENDIX A

Study Terms of Reference

TABLE OF CONTENTS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

July 13, 1998

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: National Defense Industrial Association Study on Information Assurance

The Department of Defense (DoD) has become increasingly reliant on the use of information systems to accomplish its many missions. However, such reliance creates a concomitant increased vulnerability in our operational capabilities. Additionally, as the DoD continues to move toward the use of open systems, shared databases, and commercial off-the-shelf (COTS) products, we face even greater challenges. The increasing threat to our current and future information systems may potentially outstrip those DoD resources available to provide the requisite level of information assurance.

Accordingly, in January of this year, the Information Assurance Directorate within my office requested that the National Defense Industrial Association (NDIA) undertake an independent industry study to determine if and how information assurance support in the DoD could be augmented through outsourcing to private industry. The NDIA study will focus on evaluating where industry support could assist in improving the readiness levels of critical systems through expanded monitoring, red teaming, validation testing, and system certification.

The NDIA study is currently underway and will be completed by November 1998. Mr. Fred Demech from TRW chairs the study team, which consists of numerous representatives from more than ten companies. The NDIA has an outstanding reputation for conducting quality studies for government sponsors, and its studies have been of great value to the process of formulating government regulations, policies and budgetary strategies. As a result, both government and industry have benefited from these efforts.

I strongly encourage you and your staff to support this important endeavor if members of the study team call upon you to solicit your views and advice. Should you have any questions with regard to this effort, my point-of-contact is Ms. Virginia Castor, who is assigned to the Office of the Deputy Assistant Secretary of Defense for Security and Information Operations. She can be reached via telephone at (703) 695-2666 or via e-mail at castorv@osd.pentagon.mil.

Arthur L. Money
Senior Civilian Official

TERMS OF REFERENCE

INFORMATION ASSURANCE ANALYSIS STUDY

Conducted By The

National Defense Industrial Association

Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) Committee

For The

Office of the Assistant Secretary of Defense (OASD) for Command, Control, Communications and Intelligence (C3I)

General:

The Office of the ASD (C3I) is concerned with the issue of information assurance. DoD, as well as other Federal agencies and industry, information systems have become increasingly more vulnerable to inadvertent and covert unauthorized intrusion. These intrusions threaten the effectiveness of the systems, impact the readiness of DoD to perform its missions, and have the ability to disrupt the delivery of critical services nationwide. As DoD and industry move toward more open systems, shared databases and the use of COTS, the ability to provide information assurance has become difficult. At the same time, rapid jumps in computer technology have raised the threat level by providing a means for even the novice hacker to gain access and disrupt the flow of information within critical infrastructure systems. The concern of OASD/C3I is how it will be able to provide information assurance against a rising threat that has the potential to outstrip available DoD resources to monitor and test current and new systems coming on line.

For these above reasons, OASD/C3I has requested that the NDIA C4ISR Executive Committee undertake an independent industry study to determine if the DoD/Federal Government information assurance support can be augmented through outsourcing to private industry. The study will focus on evaluating areas where industry support could improve the readiness levels of critical systems through expanded monitoring, validation testing and system certification. The specific areas that the Study will encompass are presented below in the *Terms of the Study*. The output of this proposed study will be a written report submitted to OASD/C3I for its specific use.

Proposal:

It is proposed that the NDIA/C4ISR Executive Committee undertake a study to determine the viability of outsourcing DOD's information security support to private industry. The proposed study will address the areas listed below in the *Terms of the Study* and we will document our study results in a final written report to OASD/C3I.

Study Deliverables:

The study deliverables will consist of periodic progress and status briefings to OASD/C3I and a final written report. At the conclusion of the study, the C4ISR Study Team will prepare and present a formal briefing and provide a written report documenting our approach, findings, conclusions and recommendations

Terms of the Study:

In order to ensure preparation of a fully useful assessment, analysis, and report, the study will be conducted in accordance with the terms defined herein.

1. The study will provide to OASD/C3I industry's view on the best practices that can be employed to improve the level of information assurance across the wide range of communications exchanges that occur within the auspices of DoD. Special attention will be paid to those areas that have the potential to adversely impact the readiness of U.S. Military forces and related DoD support agencies.

2. This study effort will gather statistics, analyze and catalog the methods, procedures, processes and tools that have been used to support information security within DoD and industry.

3. The study will investigate the expected protection (assessment against an increasingly, more sophisticated IT threat) requirements associated with the implementation of new systems, COTS products and increasingly diverse information distribution requirements, and evaluate the latest measures being taken by DOD and industry to safeguard the information.

4. The study will investigate methods to improve the ability of DoD to measure and test for readiness of information systems to provide information assurance, including reviewing training and testing methods and validation criteria being employed by DoD and industry.

5. The study will investigate the viability, related issues and possible implementation methods to determine if Red Team Testing and certification of DoD information systems could be outsourced to private industry.

6. As part of paragraph 5 above, the study will investigate and make recommendations on possible approaches for creating an organizational process that would provide guidance for outsourcing to industry, including addressing the following issues:
   - Industry Management of the information assurance process.
   - Establishing and approving a comprehensive set of common Best Practices
   - Determining evaluation and acceptance criteria
   - Development of testing and validation procedures to test readiness.

7. The study will record the results of DoD, related Government agencies, and industry comments and recommendations on all of the above issues and include them as part of the final report.

8. As a minimum, the data gathering efforts and study surveys will include senior DoD and Government Information Technology officials and a wide cross section of small, medium and large information technology companies.

9. It is expected that 12 to 15 members will be assigned to the Study Team, and that the study effort will be completed within 6 – 9 months from the approval date of these Terms of Reference.

10. The study will be undertaken at no cost to the Government.

11. The output of the study will be a report that addresses, at a minimum, the areas cited in paragraphs 1 through 10 above.

12. The TOR may be modified at any time by mutual agreement between OASD/C3I and the NDIA C4ISR Executive Committee.

AGREED TO:

Edwin D. Patton
NDIA/C3ISR , Chairman
Date: 1/30/98

Virginia L. Castor
Ms/Virginia L. Castor
OASD/C3I Representative
Date: 1/30/98

APPENDIX B

Best Practices of Leading Organizations

Compiled by
Douglas E. Campbell, Ph.D.,
President, Syneca Research Group, Inc.

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

CI, as the lead for the NDIA C3I Information Assurance Study, has responded to the task of "investigating the viability, related issues and possible implementation methods to determine if Red Team testing and certification of DOD information systems could be outsourced to private industry." GRCI determined that it could best serve the study by "investigating and making recommendations on possible approaches for creating an organizational process that would provide guidance for outsourcing to industry," including addressing the following issues:

Industry management of the information management process

Establishing and approving a comprehensive set of common best practices

Determining evaluation and acceptance criteria

Development of testing and validation procedures to test readiness

This Appendix to the main NDIA C3I study report focuses on four major studies in the area of "best practices" in the Information Assurance field. This Appendix provides the reader with a synopsis of:

The Organization for Economic Cooperation and Development's (OECD) *Guidelines for the Security of Information Systems*, considered in this Appendix as the baseline for generally accepted principles and practices in securing information technology (IT) resources.

A National Institute of Standards and Technology (NIST) report entitled *Generally Accepted Principles and Practices for Securing Information Technology Systems*, dated September 1996.

A United States General Accounting Office (GAO) Report entitled *Information Security Management: Learning From Leading Organizations*, dated May 1998.

The Report on *The Analysis of the Naval Safety Center as a Model for Information Warfare*. This study, in which Dr. Campbell participated, was incorporated as Appendix D of the Draft *Information Warfare Implementation Plan* written for the Information Warfare Council as part of the Department of the Navy (DON) Information Warfare Enterprise, dated 19 June 1997. The Naval Safety Center Study was originally submitted 20 January 1997.

NOTE: A Datapro report entitled *The Quest for Generally Accepted System Security Principles*, published in October 1994 may make for interesting background reading but could not be made available by the delivery date of this study.

This Appendix approaches the subject of "Best Practices" along a general-to-specific path (see Figure 1). This Appendix begins with a baseline of generally accepted principles and practices used in securing information technology resources. This Appendix ends with a very specific look at many "possible approaches for creating an organizational process that would provide guidance for outsourcing to industry."

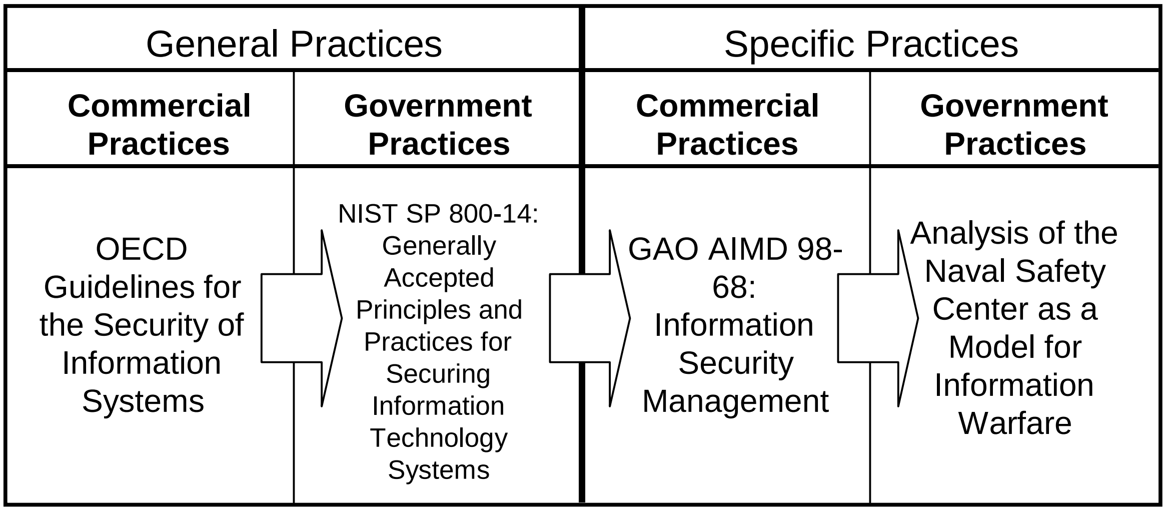

General Practices
Specific Practices
Commercial Practices
Government Practices
Commercial Practices
Government Practices
OECD Guidelines for the Security of Information Systems
NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
GAO AIMD 98-68: Information Security Management
Analysis of the Naval Safety Center as a Model for Information Warfare

Figure 1. Evolution of "Best Practices" Along a General-to-Specific Route as Reflected in This Appendix.

2. THE BASELINE FOR GENERALLY ACCEPTED PRINCIPLES AND PRACTICES.

As the heading implies, the principles are generally accepted in that these principles and practices are most commonly being used at the present time to secure information technology (IT) resources. These baseline principles are not new to the security profession. They are based on the premise that (most) everyone applies these when developing or maintaining a system and they have, by default, become generally accepted. This appendix uses the Organization for Economic Co-operation and Development's (OECD) *Guidelines for the Security of Information Systems* as the baseline for the ensuing basic principles.

The OECD Guidelines were developed in 1992 by a group of international experts to provide a foundation from which governments and the private sector, acting individually or as a team, could construct a framework for securing IT systems. The *OECD Guidelines* are the current international guidelines that have been endorsed by the United States. A brief description of the nine OECD principles is provided in Table 1.

3. THE FEDERALIZATION OF GENERALLY ACCEPTED PRINCIPLES AND PRACTICES

Using the spirit of the OECD *Guideline*s, the National Institute of Standards and Technology (NIST) developed principles that applied to Federal systems. In developing this set of principles, NIST drew upon the OECD Guidelines, added material, combined some principles, and rewrote others. Most of the rewriting and combining was done to provide clarity. The principles added by NIST are in keeping with the OECD principles but not directly stated. For example, NIST added the principle "Computer Security Supports the Mission of the Organization." Prior to developing these principles, NIST thoroughly reviewed what was currently being accomplished in the IT Security principles area. With much consideration, a determination was made that the U.S. Government would benefit from its own set of principles.

Table 1. OECD's Guidelines for the Security of Information Systems.

Accountability	The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.
Awareness	Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.
Ethics	The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.
Multidisciplinary	Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....
Proportionality	Security levels, costs, measures, practices and procedures should be appropriate and

	proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....
Integration	Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.
Timeliness	Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.
Reassessment	The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.
Democracy	The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

NIST published Special Publication 800-14 in September 1996 entitled *Generally Accepted Principles and Practices for Securing Information Technology Systems*. The eight principles contained in that document provide an anchor on which the Federal community should base its IT security programs, including the area of information assurance. These principles are:

17. Computer Security Supports the Mission of the Organization.
18. Computer Security Is an Integral Element of Sound Management
19. Computer Security Should Be Cost-Effective
20. Systems Owners Have Security Responsibilities Outside Their Own Organizations
21. Computer Security Responsibilities and Accountability Should Be Made Explicit
22. Computer Security Requires a Comprehensive and Integrated Approach
23. Computer Security Should Be Periodically Reassessed
24. Computer Security Is Constrained by Societal Factors

These principles were intended to guide agency personnel when creating new systems, practices, or policies. As principles, they are not designed to produce specific answers. The principles should be applied as a whole, pragmatically and reasonably. Each of the eight principles are expressed as a sub-heading and synopsized in the paragraphs that immediately follow. Some "wordsmithing" within the paragraphs was executed by the author to focus the reader on specific comments.

Computer Security Supports the Mission of the Organization. The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake--they are put in place to protect important assets and support the overall organizational mission. In a private-sector business, having good security is a business practice usually secondary to the need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is a business practice usually secondary to the agency's providing services to citizens. Security, then, *ought to* help improve the service provided to the citizen. Thus, Federal managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined and the subsequent business practices can be put into place. In the Federal Government, security can only be explicitly stated in terms of the organization's mission.

Computer Security is an Integral Element of Sound Management. Information and IT systems are often critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees.

However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what level of risk they are willing to accept, taking into account the cost of security controls.

As with other resources, the management of information and computers may transcend organizational boundaries. When an organization's information and IT systems are linked with external systems, management's responsibilities extend beyond the organization. This requires that management (1) know what general level or type of security is employed on the external system(s) or (2) seek assurance that the external system provides adequate security for their organization's needs.

Computer Security Should Be Cost-Effective. The costs and benefits of security should be carefully examined *in both monetary and non-monetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system.

In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its IT system. Security measures, such as an improved access control system, may significantly reduce the loss.

Moreover, a sound security program can thwart hackers and reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity.

Security benefits do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these have to be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the initial cost of the control (as is often seen, for example, in the costs of administering an access control package). Solutions to security problems should not be chosen if they cost more, in monetary or non-monetary terms, directly or indirectly, than simply tolerating the problem.

Systems Owners Have Security Responsibilities Outside Their Own Organizations. If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that the system is adequately secure. This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.

In addition to sharing information about security, organization managers "should act in a timely, coordinated manner to prevent and to respond to breaches of security" to help prevent damage to others. However, taking such action should *not* jeopardize the security of systems.

Computer Security Responsibilities and Accountability Should Be Made Explicit. The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries.

Depending on the size of the organization, the computer security program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does *not* specify that individual accountability must be provided for on all systems. For example, many information dissemination systems do not require user identification or use other technical means of user identification and, therefore, cannot hold users accountable.

Computer Security Requires a Comprehensive and Integrated Approach. Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

To work effectively, security controls often depend upon the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that if their system has been checked once, that it will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

Computer Security Should Be Periodically Reassessed. Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connection to external networks; a change in the value or use of information; or the emergence of a new threat.

In addition, security is *never* perfect when a system is implemented. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare and procedures become outdated over time. These issues make it necessary to reassess periodically the security of IT systems.

Computer Security is Constrained by Societal Factors. The ability of security to support the mission of an organization may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures may be considered invasive in some environments and cultures.

Security measures should be selected and implemented with a recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security.

The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

4. BEST PRACTICES OF LEADING ORGANIZATIONS--THE GENERAL ACCOUNTING OFFICE (GAO) STUDY.

To supplement the ongoing audit work at federal agencies and gain a broader understanding of how information security programs can be successfully implemented, the GAO studied the management "best practices" of eight non-federal organizations recognized as having strong information security programs. The specific objective of the review was to determine how such organizations designed and implemented their programs in order to identify practices that could be applied at federal agencies.

The GAO focused primarily on the management framework that these organizations had established rather than on the specific controls that they had chosen, because previous audit work had identified security management as an underlying problem at federal agencies. Although powerful technical controls, such as those involving encryption, are becoming increasingly available to facilitate information security, effective implementation requires that these techniques be thoughtfully selected and that their use be monitored and managed on an ongoing basis. In addition, there are many aspects of information security, such as risk assessment, policy development, and disaster recovery planning, that require coordinated management attention.

To identify leading organizations, the GAO reviewed professional literature and research information and solicited suggestions from experts in professional organizations, nationally known public accounting firms, and federal agencies. In selecting organizations to include in their study, the GAO relied primarily on recommendations from the Computer Security Institute and public accounting firms because they were in a position to evaluate and compare information security programs at numerous organizations. In addition, the GAO attempted to select organizations from a variety of business sectors to gain a broad perspective on the information security practices being employed. After initial conversations with a number of organizations, the GAO narrowed their focus to eight organizations that had implemented fairly comprehensive information security programs across their respective organizations. All were prominent nationally known organizations. They included a financial services corporation, a regional electric utility, a state university, a retailer, a state agency, a non-bank financial institution, a computer vendor, and an equipment manufacturer. The number of computer users at these organizations ranged from 3,500 to 100,000, and four had significant international operations. Because most of the organizations considered discussions of their security programs to be sensitive and they wanted to avoid undue public attention on this aspect of their operations, the GAO agreed not to identify the organizations by name.

The GAO obtained information primarily through interviews with senior security managers and document analysis conducted during and after visits to the organizations they studied. In a few cases, they toured the organizations' facilities and observed practices in operation. They supplemented these findings, to a very limited extent, with information obtained from others. For example, at the state agency, they also met with a statewide security program official and with state auditors. In addition, the GAO asked the Computer Security Institute to query its members about their efforts to measure the effectiveness of their security programs in order to gain a broader perspective of practices in this area.

To determine the applicability of the leading organization's practices to federal agencies, the GAO discussed their findings with numerous federal officials, including officials in OMB's Information Policy and Technology Branch, the Computer Security Division of NIST's Information Technology Laboratory, CIO Council members, the chairman of the Chief Financial Officers Council's systems subcommittee, information security officers from 15 federal agencies, and members of the President's Commission on Critical Infrastructure Protection. Further, they discussed their findings with our Executive Council on Information Management and Technology, a group of executives with extensive experience in information technology management who advise us on major information management issues affecting federal agencies.

Throughout their document, they made several observations on federal information security practices in order to contrast them with the practices of the non-federal organizations that they studied. These observations were based on the body of work they had developed over the last several years and on their recent discussions with federal information security officers and other federal officials who are knowledgeable about federal information security practices. Although they attempted to be as thorough as possible within the scope of their study, they recognized that more work in this area remains to be done, including a more in-depth study of individual practices. They also recognized that the practices require customized application at individual organizations depending on factors such as existing organizational strengths and weaknesses.

The GAO effort recognized a total of five major principles in which existed 16 practices. The summary of their effort can be seen in Table 2.

Table 2. A Summary of Sixteen Security Practices by Leading Organizations

PRINCIPLES	PRACTICES
Assess Risk and Determine Needs	1. Recognize information resources as essential organizational assets 2. Develop practical risk assessment procedures that link security to business needs 3. Hold program and business managers accountable 4. Manage risk on a continuing basis

Table 2. A Summary of Sixteen Security Practices by Leading Organizations (Continued)

PRINCIPLES	PRACTICES
Establish A Central Management Focal Point	5. Designate a central group to carry out key activities 6. Provide the central group ready and independent access to senior executives 7. Designate dedicated funding and staff 8. Enhance staff professionalism and technical skills
Implement Appropriate Policies and Related Controls	9. Link policies to business risks 10. Distinguish between policies and guidelines 11. Support policies through central security group
Promote Awareness	12. Continually educate users and others on risks and related policies 13. Use attention-getting and user-friendly techniques
Monitor and Evaluate Policy and Control Effectiveness	14. Monitor factors that affect risk and indicate security effectiveness 15. Use results to direct future efforts and hold managers accountable 16. Be alert to new monitoring tools and techniques

5. BEST PRACTICES OF A SUCCESSFUL GOVERNMENT ORGANIZATION--THE NAVAL SAFETY CENTER, NORFOLK, VA.

The purpose of the study was to refine the management of Space & Naval Warfare Command's (SPAWAR's) PMW 161 (Information Warfare-Defense, or IW-D) Information Security plans, goals, milestones and metrics. To do this, a search was performed to find any successful programs outside the Information Warfare field in which those successes could be transferred to SPAWAR. The search produced the successful role that the Naval Safety Center has played in the Department of Defense. The original study was prepared by CORBETT Technologies, Inc., of Alexandria, VA, under contract to Booz, Allen & Hamilton, Inc. Participants of the study were Mr. Barry Stauffer, Dr. Frank Pittelli and Dr. Douglas Campbell. For brevity's sake, the R&M portion was removed and some background information was also eliminated. However, the main "best practices" are well established. There are some very pertinent recommendations and conclusions in this study to warrant a close look at "best practices" that could be used in Information Assurance.

Given the time and resource-sensitive nature of this effort, a “Quick Look” methodology was used to examine the management procedures and metrics used in the Naval Air Training and Operating Procedures Standardization (NATOPS) manuals, Naval Air Safety, and Reliability & Maintainability (R&M) programs and to determine their applicability to the Navy IW-D programs. The “Quick Look” methodology included as its first step the high-level review of the current Navy IW-D acquisition and management procedures and management of active IW-D programs. This high-level review examined the IW-D management procedures to understand how goals, plans and milestones are developed and monitored.

The second step performed a high-level review of the NATOPS, Naval Air Safety, and R&M programs. All three programs were reviewed only to determine how these successful programs are managed, i.e., how their goals, plans, and milestones are developed, and how the results are measured. Specifically, this review collected and subsequently analyzed the use of metrics to monitor and report progress. Key Navy staff familiar with these three programs were interviewed and various documents examined to provide the necessary information for review.

The third step compared the results of the review of the IW-D analysis with the review of the three Navy programs. This comparison applied only to the development of goals, plans and milestones, and the use of metrics, within the three Navy programs studied, and the applicability of those areas to the Navy's IW-D program.

The fourth and final step was the creation of this report, summarizing the results and findings of the comparison. The report concludes with recommendations related to management procedures and metrics used in the NATOPS, Naval Air Safety, and the R&M programs could be successfully transferred or reengineered into the Navy's INFOSEC and IW-D programs.

5.1 Overview Of The Naval Air Safety Program

The Naval Air Safety Program is an operational program with key responsibilities vested in operational units, or the “Fleet,” and with program support from the safety staff. The operational units are supported by the Naval Safety Center (NSC), headquartered in Norfolk, VA, and the Safety School at the Naval Postgraduate School (NPS) located in Monterey, CA.

The operational component the program is managed by RADM McGinn, N88, Air Warfare Division. The safety component is led by RADM Dirren who is on the staff of the Vice Chief of Naval Operations, as the Special Assistant for Safety Matters, OPN09F. This dual functionality is carried downward directly to the key department heads at the squadron level. These department heads are: the Squadron Operations Officer who is responsible for flight operations and scheduling; the Maintenance Officer who is responsible for aircraft maintenance and ground operations; and the Safety Department Head who manages the Aviation Safety Program, NATOPS and ground safety. All three report directly to the Squadron Commanding Officer (CO), who has the ultimate responsibility for squadron operations and safety.

At the squadron level, each squadron has a dedicated safety officer who manages the squadron safety program under the direction of the squadron CO. The NSC provides support as discussed below. The Safety School provides the required education for all prospective squadron CO's and Safety Officers.

Although it is difficult to precisely state which changes caused which improvements, it is correct to state that overall safety has improved significantly as a result of the focus provided by the Safety Program. It is hoped that some of the lessons learned and the techniques developed by the Safety Program can be used to strengthen the INFOSEC and IW programs, as they are required to mature in a shorter period of time.

At its infancy, the Safety Program was apparently neither liked nor respected. Many operational commanders felt that safety requirements were a "tax" on their operational goals and did not see a real value wholehearted support. Now, over 40 years later, the Safety Program itself is completely an operational program, in which the key responsibilities are vested in operational units with program support and advice from staff organizations like the NSC and the Safety School at the Naval Postgraduate School. The fleet is responsible for all safety issues and has the authority and accountability that goes with such responsibility. The support organizations assist in the management of the Safety Program and provide a source of expert advice for both pro-active and reactive safety issues.

The degree to which safety has been accepted by the operational units can be seen in the key roles that have evolved to facilitate the program, as well as in the information that flows regularly throughout the Navy to increase safety. Regardless of the "cause-and-effect" of a NSC having direct or indirect influence on reducing the loss of aircraft and loss of life per 100,000 flight hours, it is important to see that the naval aviation mishap rate has been overall dropping since Fiscal Year 1950. Various actions have taken place that may have directly or indirectly influenced the continuing reduction of such mishaps. These actions include:

Angled decks on aircraft carriers

Establishment of the NSC in 1953

Establishment of the Naval Aviation Maintenance Program in 1959

Initiation of the Replacement Air Group (RAG) Concept in 1959

Initiation of the NATOPS Program in 1961

Initiation of the Squadron Safety Program in 1978

System Safety Designated Aircraft in 1981

Initiation of Aircrew Coordination Training (ACT) in 1991

5.2 Information Flow

In addition to the roles and responsibilities assigned to individuals, one of the best methods for determining how a process or program is implemented is by examining the formal and informal flow of information between all of the participants. In the Safety Program, this flow of information is formalized by the following reports:

Mishap Report
Hazard Report (HAZREP)

5.2.1 Mishap Reports

Whenever an aviation incident occurs, a Mishap Report is filed and categorized as follows,

Category	Personnel Loss	Equipment Loss
Class A	Loss of Life	Over $1M

Category	Personnel Loss	Equipment Loss
Class B	Partial Disability	Between $200K and $1M
Class C	5 or more work days	Between $10K and $200K

Mishaps are as defined in OPNAVINST 3750.6. The definition as to which class should be assigned is not subjective. In fact, the formulas for calculating equipment loss and determining "lost work days" is precisely defined and leaves very little room for interpretation.

The purpose of these reports is to "accurately" document losses due to safety incidents, to help prevent such problems in the future. To that end, following each mishap or near-miss incident, a safety board is convened to identify the factors that caused the mishap. The members of this board are well defined in the OPNAVINST, but vary with the class of mishap. A representative from the Safety Program is available for expert advice and to help determine the cause of the problem.

Following the investigation of each mishap, a detailed report is finalized by the NSC and sent to every unit that operates or maintains that aircraft. There are also recommended corrective action messages that are again sent to units that own or operate the aircraft. Generally, each message contains 2-3 corrective actions. There are approximately 200-300 such messages sent per year.

All Mishap Reports are permanently maintained by the NSC in a database that is used for a range of safety-related activities.

5.2.2 Hazard Reports

Hazard Reports (HAZREPs) are filed whenever any individual or organization feels that a potential safety problem exists or there is a risk of such a problem occurring. Generally, there are 10-20 times as many HAZREPs as Mishap Reports, covering a wide range of issues. HAZREPs are broadcast throughout the Navy to any organization that has an interest in the topic being addressed. HAZREPs may or may not cause action to be taken, depending on the issue and the severity of the problem.

HAZREPs, by their nature, are more subjective and include such things as "close calls." Although the investigation of HAZREPs is not formalized, they are extremely useful in detecting problems before they happen. Some number of HAZREPs may never yield any new useful information, but it is "better to be safe than sorry." HAZREPs are recognized by the fleet as a common tool for informing the chain of command and fellow sailors about potentially dangerous situations. Anyone can submit a HAZREP and their use is encouraged.

There are also non-hazard reports that are written, and submitted. These reports document deficiencies, such as lost tools, in the form of Loss Tool Reports, Equipment Improvement Reports, etc. These reports are usually originated by the logistics or maintenance staff. If need be, and if resources are available, one could collect all these reports to research new procedures or trends, study the reliability of tools, the provider of tools, etc.

All HAZREPs are permanently maintained by the NSC in a database that is used to support a range of safety-related studies and activities.

5.3 White-Hat Approach.

It is extremely important to note that the NSC plays a "white-hat" role in all areas regarding safety. That is, they exist to provide advice and to assist in the management of the Safety Program. The NSC does not assign blame, nor are they responsible for directly ensuring safety throughout the fleet. The NSC performs safety visits, with the safety teams spending six months of a year on the road performing such visits. These are non-attribution visits in that the team comes in, audits safety, reports their findings to the Safety Officer and CO, and then "burns the notes." Whenever the NSC participates in a mishap investigation, their only purpose is to determine the actual cause, regardless of any personnel actions proceeding in parallel by other organizations, like the Judge Advocate General's office (JAG). To that end, the NSC has the authority to keep specific information confidential, if so requested by an individual. Over the years, this authority has been consistently upheld at the highest levels of the Navy and by the U.S. Supreme Court. Consequently, all personnel know that they can speak freely to NSC investigators and critical safety-related information can be acquired. According to all of the people interviewed, this is one of the most critical aspects of the NSC's role and is a significant reason for their success over the years in determining the true cause of safety problems.

The importance of obtaining accurate mishap information cannot be overstated. Mishap reports, when initially submitted, may not provide a complete picture of the incident. Trained, expert investigators from the NSC help to clarify the key issues and to determine the most likely cause. As such, when the Mishap Report is completed and added to the NSC's database, it represents an extremely valuable piece of information for further study, which in the future may help predict potential problems.

Based on the degree to which the NSC has been accepted into the day-to-day activities of the fleet, as demonstrated by the following list, it is evident that the NSC has successfully staved off the image of "Safety Cop" and is now truly "trusted" by the fleet.

5.4 Program Management.

Within the Naval Air Systems Command (NAVAIR), each aircraft type is assigned to a program management office (PMA). This PMA is responsible for all aspects of the aircraft from cradle to grave. The PMA monitors all equipment and maintenance problems. (Note: severe maintenance problems could be elevated to increased attention if they are deemed to pose safety problems.)

There are a number of closely related programs. These include:

Naval Air Training and Operating Procedures Standardization (NATOPS) program. This is a fleet administered program for each aircraft type. The NATOPS program focuses on training and standardization of procedures. A NATOPS Manual exists for each aircraft type. These manuals define the function of all aircraft and ground equipment. Instructions directly related to safety are surrounded by a bold red border. The NATOPS program is the core of all aircrew training. The program involves frequent tests and reviews at each level of proficiency. NATOPS instructors frequently accompany the crews on flights to provide standardization assistance. There is an annual NATOPS conference to review proposed changes to the manual. The Safety Center NATOPS representative for that aircraft type attends these meetings and is a voting member. During these conferences, NAVAIR retains control over all procedures that relate to the aircraft performance envelope. All other procedures are voted upon by the fleet representatives.

Naval Occupational Safety and Health (NAVOSH) is primarily focused on ground safety matters. The mission of NAVOSH is to provide quality education and training, and associated services, for all military and civilian Navy personnel, afloat and ashore, in the areas of occupational safety and health, and environmental protection. The intent is to enhance operational readiness at all levels and echelons to preserve safe and healthful workplaces, while protecting and restoring the environment.

Quality Assurance (QA). There are QA personnel at all levels of the aviation maintenance program. The staff inspects all aircraft work and carefully monitors trends, such as lost tools, which become secondary indicators of potential safety problems.

Safety-related Reports. There are several report types that while not directly related to safety, support the overall program and the improvement of safe effective procedures. These include Hazardous Material Reporting, Equipment Improvement Reports, and Document Improvement Reports

5.5 Naval Safety Center Mission And Functions

5.5.1 Mission

The mission of the NSC is: "...to enhance the war fighting capability of the Navy and Marine Corps by arming our Sailors, Marines and civilians with the knowledge they need to save lives and preserve resources. Of interest here is that the NSC has as its mission to "enhance the war fighting capability" using "knowledge" as its only armament. The same could be said about all three areas of Information Warfare (Attack, Exploit, Defend) in that it is the increased knowledge that must be provided to the IW environment that will save lives and preserve resources.

As a member of the CNO staff, the Commander of the Safety Center represents the CNO on all matters related to safety. In this role the Safety Director, OP09F, manages the safety program and issues the Navy Safety instruction OPNAVINST 3750.6. The Safety Center defines program goals, how to investigate mishaps, who investigates, and the qualifications of the investigators.

5.5.2 Functions

From the NSC perspective, “knowledge” takes many shapes. The NSC assists the CNO in managing all aviation, afloat and shore safety programs. This is accomplished by the following:

Supporting many and varied program areas (aviation, surface ships, submarines, diving, occupational safety and health, motor vehicles, explosives and weapons, fire protection, environmental, recreational, off duty, and high risk training safety).

Collecting and providing safety data. NSC is the repository for all collected safety data. They perform analysis on such data and respond to requests for such data.

Participating in safety visits. NSC participates in safety surveys, safety stand-downs, maintenance malpractice, and mishap investigations. They assist the Inspector General and hold a seat on several boards and committees, including the INSURV Board.

Hazard awareness products. NSC produces and distributes the bimonthly *Approach* magazine and various safety-related newsletters; attends and participates in conferences and seminars; and publishes checklists, bulletins and messages.

5.5.3 Goals

The NSC has defined 15 goals. Exactly how they are to achieve each goal is currently under investigation by the NSC, pending availability of resources, but the conscious act of writing them down is a step in the right direction. These 15 goals are as follows:

1. Develop a sense of ownership for our mission, vision and strategic plan.

25. Improve our methods of collecting and analyzing data.

26. Standardize the quality of safety programs in the aviation, shore and afloat directorates.

27. Ensure our staff is well-trained.

28. Improve communications with our customers.

29. Increase the NSC's participation in policy-setting groups.

30. Pursue new ideas.

31. Market risk management as a part of everyday life.

32. Exploit the use of all media. Identify our target customers.

33. Better manage our resources.

34. Foster trust and openness in our relationships with our customers.

35. Establish the most effective NSC organization that best enhances our ability to anticipate and respond to customer needs and improve the safety process.

36. Have the Commander, NSC, designated as the Director of Naval Safety.

37. Pursue a new marketing strategy.

38. Make our customers more knowledgeable.

5.5.4 Guiding Principles

The NSC team exists to assist the naval forces (identified as their "customers"). In their dealings with these customers, the NSC is guided by the following principles:

Be honest and cooperative and treat all customers with dignity and respect.

Make sure our customer's needs come first.

Continuously improve.

Serve as consultants and advisors, enabling our customers to recognize hazards and manage risks.

To ensure that these guiding principles are met, the NSC supports their own personnel by:

Allowing them to exercise authority at the lowest level;

Promoting open communications;

Encouraging teamwork; and,

Stimulating and supporting professional development.

5.5.5 Safety Awareness

The Safety Awareness program is the key NSC program. The Awareness program includes:

A bimonthly safety magazine (*Approach*) directed toward the aircrews.

Quarterly reviews by aircraft type.

Monthly messages.

Mishap reports to collective addresses.

Squadron Safety Stand-down support.

The Director of the NSC speaks to every command class (One-week safety class for aviation CO's and the CO class for ships.)

5.5.6 Process Improvement

The NSC has a Process Action Team (PAT) which is reviewing the way the NSC manages the safety program. The NSC is moving toward the use of "Trip Wires" which will alert them when certain events occur.

5.6 Training

The key safety training is performed by the School of Aviation Safety at the Naval Postgraduate School. The command level and aviation safety officer training courses are offered only at the School of Aviation Safety. A conference is held once every two years (with Naval Safety Center personnel attending) so that the curriculum can be reviewed and the curriculum updated, if necessary.

The mission of the School of Aviation Safety is: To educate aviation officers at all levels; to identify and eliminate hazards, to manage safety information, and to develop and administer command safety programs; to foster and conduct safety-related research; and to provide assistance in support of the Naval Aviation Safety Program; thereby enhancing combat readiness through the preservation of assets, both human and material.

5.6.1 Command Level Course

The five-day Aviation Safety Command (ASC) course is offered eight times each year at the Naval Postgraduate School in Monterey, CA. The ASC course is offered to Navy and Marine commanding officers, executive officers, officers in charge of aviation detachments, officers screened for command and staff officers in the rank of Lieutenant Commander, or Major, and above. This course is designed to provide information which will assist commanding officers in conducting an aggressive mishap prevention program and to prepare the graduate for the duties of Senior Member of a Mishap Board. The course consists of approximately 35 classroom and laboratory hours over five instructional days, addressing subjects including safety programs, safety psychology and human factors, aviation law, aircraft systems, mishap investigation techniques, mishap and incident reports and endorsements and aerospace medicine.

5.6.2 Safety Officer Course

The 28-day Aviation Safety Officer (ASO) course is offered seven times each year, on a temporary additional duty basis, for those commands needing an Aviation Safety Officer. This course prepares the graduate to assist his or her commanding officer in conducting an aggressive mishap prevention program. When the ASO completes the course, he or she will be able to organize and administer a mishap prevention program at the squadron level as defined in OPNAVINST 3750.6. This 28 instructional-day course consists of approximately 160 classroom and laboratory hours. Subjects addressed include safety programs, risk assessment and mishap prevention techniques, operational aerodynamics and aerostructures, mishap investigation and reporting, psychology, human factors, safety law and aeromedical support. Designated naval aviators and naval flight officers of the Navy and Marine Corps in the rank of Lieutenant, (USN) and Captain, (USMC) and above are eligible to attend.

5.6.3 Additional Courses

Aviation squadron personnel receive safety training at many levels. The airman is introduced to safety training in many stages as he or she prepares for the first assignment. The aviator has safety training emphasized at each stage of their training from Preflight to completion of the aircraft specific training. By the time a replacement arrives in a squadron, they have a firm foundation of safety training.

5.7 Squadron CO Perspective

There are training, tools and benefits present that clearly demonstrate that naval air safety has become ingrained in the career development/career enhancement of every naval aviator, from Airman to Admiral. The perspective can be seen at the Squadron Commanding Officer level in the formal training available to the CO and his/her staff. The CO also has a myriad of tools available at the their disposal. The CO's understand the benefits to them and the squadron from using such tools and participating in the safety program. The formal training has been discussed above. This training is supplemented by the squadron-level programs and the NATOPS programs in the squadron. There are frequent reviews and check flights for the crew members and inspections or reviews for the squadron. If a CO feels the need for additional assistance, he or she can request a visit from the NSC.

Squadron safety records are viewed as critical information in the evaluation of the squadron CO. A weak or poor safety record is not career enhancing. Conversely, the periodic squadron safety competition and awards are strong motivators for all members of the unit.

5.8 Findings

The purpose of this study was to determine those areas of "best practices" within the Safety Program that ***may*** serve as templates or analogies for strengthening the Security Program. Whereas more detailed study is needed to properly determine if, in fact, the analogies hold and/or similar results will be possible, here we make some high-level observations about the Safety Program's success and draw some tentative relationships to the Security Program.

The success of the Safety Program appears to stem from the following fundamental characteristics:

- Over 40 years of evolution.
- Clear assignment of responsibility, authority and accountability to operational commanders.
- Free flow of incident and preventative information to all organizations that have a vested interest in that information.
- "White-Hat" approach to gathering information and assisting with reviews, both pro-active and reactive.
- Existence of a database of all safety-related reports, maintained by safety experts and used for a wide-range of purposes.
- Coordinated training across all ranks and specializations.

As indicated in the first bullet, success has not come quickly or easily. The Safety Program has continually evolved a role that works effectively to assist operational commanders, without usurping their authority. Whereas the information and focus lies with the Safety Center, the responsibility and authority still lies with the operational commanders. The INFOSEC and IW programs are in their infancy, relatively speaking, and they would be well served by "developing" a similar role with operational commanders. Thus:

A Security Program that views the operational commanders as "customers" may be the only program that can hope to achieve the same level of acceptance that has been attained by the Safety Program.

5.8.1 Visibility And Access

Without high-level visibility and access, the NSC would not be able to gather the necessary information, or provide advice to those who can make a difference. To that end, the Safety Center reports directly to CNO, being run by RADM Dirren who is on the direct staff to CNO, OP09F. Similarly, at the squadron level, the Safety Officer reports directly to the CO.

If a similar chain of command were implemented for the INFOSEC and IW programs, the same level of visibility and access would probably result. This would provide those programs with the necessary relationships to gather and disseminate information, and to help build the level of "trust" that the Safety Program has attained. It is possible that the Security Program will never achieve the same level of trust, because it may not be possible to convince the average sailor that information security is a "life-threatening" issue. However, without high-level visibility and access, it is almost certain that the Security Program will not be accepted by the fleet.

How did the safety issue get elevated to its current importance? First, the Safety Program had to gain respect within the different communities. Initially, there was little visibility and the underlying thought was probably that safety was counterproductive. That is no longer true. Safety is now perceived as an important "operational" issue by the commander, because it helps preserve assets.

The increase in safety importance and acceptability came about during the mid 1970's and 1980's. The Marine Corps were the first to adopt it, followed by the Navy. The Safety Officer was elevated to a Department head level, giving him direct access to the Commanding Officer. Although not considered a "key" career-enhancing billet, it is a department head billet all the same.

Safety also became a public issue during and after the Vietnam War. The NSC kept track of, and documented, losses. From those statistics the NSC was able to recommend solutions to make things and people more safe. The NSC was able to identify the problem AND advise operational commanders how to fix the problem. After a sustained period of benefits were shown, the Safety Program was finally recognized as a valuable source for such information and authority soon followed.

The Security Program must emulate this approach of showing positive, tangible benefits to their customers, the operational commanders. Then, slowly but surely, they will be able to make a significant impact on the overall security of the Navy and will gain the respect that is needed to ensure acceptance by the fleet.

The major difference between safety and information warfare is that safety has the visibility--they have the "smoking hole" after an aircraft accident. The "smoking hole" is a quantifiable level of destruction with possible deadly results. In the INFOSEC/IW-D community, there may not even be an audit log available to prove that an unauthorized user had entered a computer system, or that there had been any intentional or unintentional corruption of data. Similarly, it is well understood that the most significant threat to most AIS are the insiders. These authorized users could glean information and disclose this information to unauthorized sources for years before they are detected.

The INFOSEC/IW-D community needs to focus their attention on the severity of the problem and the potential or real losses that can occur. Once the commander is convinced that the loss or compromise of their information intensive systems has resulted in the "loss" of their ship or aircraft during a Fleet Exercise, then the community may have achieved the desired visibility needed. Thus:

Elevating the visibility of IW-D within the Navy to a level comparable to that of Safety, could provide the necessary access.

5.8.2 Advisory Role

The NSC role is informational, not authoritative. The NSC is responsible for writing and maintaining OPNAVINST 3750.5, The Naval Air Safety Program. The NATOPS program is a Fleet run program that is supported by the NSC. The NSC recognizes the need to standardize and has assigned a NATOPS representative for each aircraft type. However, the Fleet owns the NATOPS manual and as such they are allowed to rewrite it. NAVAIR controls procedures related to the aircraft performance envelope, but the procedures (i.e., the different ways to operate inside the engineering data box) can be changed by the fleet operators. These changes are coordinated on an annual basis at the NATOPS conference. All this is done with NSC working with the NAVAIR and treating the fleet as the customer.

This "White-Hat" approach should definitely be given serious consideration by the Information Warfare community. For example, "Red Teams" should be viewed by the ship or shore establishments as a group that can help them in meeting their own responsibilities, instead of being viewed as another inspection team created to cast blame. (Perhaps the name, "Red Team" needs to be changed to "IW Assist Team" emphasize the role of assistance.) The Red Team reports should be delivered and held in confidence in a manner similar to that of the NSC assistance visits. The IW community needs to make their expertise available without dictating solutions to operational elements. If security is truly beneficial and the IW community truly provides a net benefit, then the operational commanders will find a way to make use of their services. Thus:

Foster a role of assistance rather than of enforcement.

5.8.3 Accurate And Timely Information

The NSC collects and analyzes all safety data (850 different attributes), even classified data, but they sanitize and publish everything open source. They are very pro-active in releasing everything they find back out into the community, with the hope that the information (e.g., which caused a Class A mishap) would assist everyone else in the Navy by preventing similar incidents from happening to them. In the Information Warfare community, it seems that incidents (e.g., insider incidents, or hackers successfully entering a network, etc.) are held in confidence and only released to a minimum number of people. Information Warfare seems to be a closed environment, and is not operating in a way that would help others prevent the same failure from happening to them. For example, threat and vulnerability information generated by the defense department is routinely labeled "No Contractor," while we expect our integration contractors to build systems that will support the Navy's needs.

The database maintained by NSC for Mishap and Hazard Reports is a critical piece of the "scientific approach" pursued by the Safety Program. Mishap Reports represent the final word on "what actually happened" during an incident, and form the basis for both reactive and pro-active activities. On the other hand, HAZREPs are more like: "this happened to us, watch out." In either case, all reports are disseminated widely so that everyone can benefit from the information contained therein. For example, a HAZREP could include information about the different Very High Frequency Omni-directional Range antennas (VORs) in Europe. There is a Class Action Designator for all aircraft that is used to broadcast that information to that particular aviation community.

This open approach is taken because, more likely than not, the information contained in one report will trigger a pro-active response by someone in the fleet. Whereas the experts at the NSC analyze information for a wide-range of reasons, individuals throughout the fleet are attuned to their unique situation and needs. Sometimes, a problem reported in one area can spark the concern of one of these front-line individuals, who may then be able to avert a potential problem. Here again, it is extremely difficult to prove that a given piece of information prevented a future problem, but the continuous improvement in safety speaks for itself.

This aspect of the Safety Program is perhaps the most controversial with regard to security. Historically, security information was "held close to the chest" because many felt that it would lead to an increase in exploitation. In recent years, security experts have reached the conclusion that if the incident information were more widely disseminated, then fewer exploitations would occur, because many problems are the result of previously known vulnerabilities. This debate will continue for some time in the security community, but the IW community needs to start forming appropriate information flows now, in order to gain benefit from that information in the future. In many respects, it is easier to lock down the information flows later, if the data contained therein is too sensitive, then to create the information flows in the first place.

Regardless of who actually sees what information, it is extremely important to note the mechanisms used by the Safety Program to disseminate information, which is based primarily upon the type of equipment being used and the mission of a given squadron. By substituting "computer type" for "airframe type," and "system administrator" for "maintenance officer," it is clear that the operational chain of command for computer systems is roughly equivalent to that for aviation equipment. To that end, it seems plausible to disseminate security information along those lines, in the same way safety information is disseminated. Thus:

Availability of accurate and timely threat and vulnerability information could help the Navy fleet-support-contractor team in achievement of Navy goals.

5.8.4 Non-Attribution Analysis

The Mishap Board is officially non-attribution because the interest lies in what needs to be done so that this mishap would not happen again, no matter who was at fault. The gathering process, as well as the reports themselves, represents a scientific approach, which gives everyone more respect for the process. (Note: a factor included in the gathering of data for such a board is the command safety atmosphere or morale. This is just another indicator of why something may have gone wrong.)

It is important to remember that accurate safety information is gathered only because of the respect afforded the NSC because of their "White-Hat" approach: determining the actual cause of the incident is their only goal. If the INFOSEC and IW community can develop the same focus, they should also be able to develop an accurate, and therefore valuable, database of security information against which scientific approaches can be used to increase overall security.

There are three different categories of mishaps based on non-subjective factors of dollars or people. Hazard Reports (HAZREPS) on the other hand, are more subjective and includes such things as "close calls." There are also non-hazard reports that are written and collected and submitted. These document deficiencies, such as lost tools, in the form of Loss Tool Reports, Equipment Improvement Reports, etc. These are usually written up by Logistics or Maintenance (4790 is the Maintenance "Bible"). If need be, and if resources are available, one could collect all these reports to research new procedures or trends, study the reliability of tools, the provider of tools, etc.

There is a 20:1 ratio between the Mishap Database and the HAZREPs (according to NAVAIR) and a 10:1 ratio according to the NSC. The Mishaps are based on what actually happened; the HAZREPs are more like: "This happened to us, watch out." The HAZREPs are collected and then distributed to everyone else needing to know this type of information. For example, a HAZREP could include information about the different VORs in Europe.

There is a Class Action Designator for all aircraft so that we know what reports to resend out to that particular aviation community. NSC is also involved in operational risk management. Based on all the reports coming in, we can suggest the best answer to reduce such mishaps or potential mishaps (Change the hardware) down through other suggestions like provide protective equipment and training. Thus:

Conduct rigorous, non-attribution analysis of significant incidents and provide responsive feedback to the fleet.

5.9 Recommendations And Conclusions

The premise of this study was the hypothesis of similarities between management of the Navy's INFOSEC and IW programs and the management of the Naval Air Safety, NATOPS and R&M programs. This study was intended to perform a high-level review of these Navy programs to determine if there were management lessons to be learned and if those lessons could be applied to the INFOSEC and IW programs.

During the course of the study we interviewed experts from the Naval Air Safety, NATOPS and R&M communities and reviewed documentation describing those programs. In addition to the general management approach we were searching for procedures related to management goal setting, measurement of progress, and the use of metrics.

The study discovered a number of areas where the Naval Air Safety, NATOPS and R&M communities differ from the IW-D community. In particular, the Safety and NATOPS programs have complemented each other to have a significant impact on the Naval Aviation management, operational and procedures. The result has been a sharp reduction in aviation incidents since the start of these programs. These communities are continuing to look for ways to get to the next level with their PAT and Risk Management processes.

The following recommendations are provided to assist in the identification of actions which could be successfully "ported" to the IW community. Each recommendation may require some additional research and analysis to determine the best way to adapt those features for the IW community.

5.9.1 Recommendations

5.9.1.1 Goals

Develop goals for the IW-D program similar to those of the NSC. Examine the NSC 15 goals and adapt their strategies and their desired outcomes to correspond with what the Information Warfare community goals and strategies.

5.9.1.2 Visibility And Access

Elevate the visibility of IW-D within the Navy to a level comparable to that of Safety. If the Security Program is to attain the same degree of success as the Safety Program, then the IW programs must have the same visibility and access. However, such a high-level position can only be effective if the operational commanders truly accept the responsibility for implementing "their own" security programs, with the assistance of a Security Program support organization. With this elevation in visibility, an awards program should be considered. Awards help to increase the visibility of any initiative among the rank and file. Like a Safety Award competition, an INFOSEC or IW-D Award competition could be implemented.

5.9.1.3 Strength Through Knowledge

Collect and analyze metrics on Navy INFOSEC incidents; develop a collection and reporting structure similar to that of the safety community; provide prompt feedback to all units with equipment similar to that involved in the incident; and invest in an effective Public Relations campaign. The perspective of using "knowledge" to increase the war fighting capability of the Navy and Marine Corps could be assumed by the Information Warfare community. Some IW-D community member could concentrate on collecting and being the repository for all collected IW data. Of primary interest is the collection of accurate security incident reports, similar to the Mishap and Hazard Reports used in the Safety Program. A formal report should be generated once a given loss threshold is exceeded and an informal report that can be generated by anyone who wants to report something "unusual" or potentially dangerous. The current incident reporting program should be examined to determine if it is effective and could support a structure similar to that of safety incident reporting.

The information gathered could also include security metrics and would include data collected from network monitoring devices, firewalls, routers, system operators, systems administrators, AIS security officers, etc. Such information would be invaluable, not only for security purposes, but to assist commanding officers in the management of their own resources. Commanding officers could determine for themselves how much effort is "typical" for their peers and could act accordingly, without the fear of being "ranked" against some metric defined by a support organization. In short, the information database should contain whatever the operational commanders think is necessary for them to conduct their own security programs.

NSC is on the Internet's World Wide Web (WWW) as part of its Public Affairs efforts. A search of WWW has found many IW-D documents being placed on there by academia, government and the public. There should be no reason to hide the efforts of the SPAWAR's IW-D efforts. Rather, SPAWAR should become pro-active in getting the word out as to what they do and what they plan to do. An Information Warfare community could produce and distribute various IW items of interest, from posters warning the sailor not to bring in their own floppy disk without having it first checked for viruses to more formal newsletters; attend and participate in conferences and seminars; and publish checklists, bulletins and messages. A responsibility of a Public Affairs Office is to track and report on the history of the command it serves. Events that were meant to reduce successful Information Warfare attacks should be tracked by SPAWAR for at least historical purposes. The history of the NSC goes back nearly 50 years; SPAWAR's role in IW goes back only a few short years and has the opportunity to put a Public Affairs Office in place generally for IW and specifically for IW-D.

5.9.1.4 Provide Expert Advice

Establish a functional equivalent to the NSC for IW-D, and adopt a similar role for the center, providing assistance to support the fleet war fighting capability. Given a central focus for such information, similar to the Safety Center, a cadre of experts could be developed to assist in the analysis and dissemination of the security information to those fleet elements to which it applies. The IW-D center should be provided the support necessary to ensure that IW-D is a well-established functional responsibility of the unit where it is located.

The NSC uses statistics to measure and verify trends. They are currently evaluating the use of trends to provide "trip wires" to warn of impending problems. The most common metric used at the NSC is the number of Class A mishaps (loss of aircraft/loss of life) per 100,000 flight hours. The NSC's statistical database contains 850 attributes drawn from all the reportable data required in OPNAVINST 3750.5. From that, trends and statistically significant events can be tracked and reported. Similar analysis could be possible for security-related information. The Naval Safety Center collects data on some 850 attributes, whereas only small amounts of metrics/statistics are collected by various information warfare communities such as DISA and NAVCIRT. The majority of these statistics are on virus hits, virus types, etc. There is a need to capture relevant statistics on the performance of computer systems throughout the Navy, at all classified levels. Network monitoring tools may be used to capture pertinent data (e.g., before and after firewalls are put in place). What is important is not only the collection of such statistics but the storage of same so that historical trends can be measured as additional statistics are collected. Also, neither DISA nor NAVCIRT can assist anyone with the actual software patch code to fix their problems. Not only should SPAWAR consider participating in evaluating such incidents, but should consider being the acquisition agent for supplying the corrected code to their users.

The Information Warfare community could also develop the elements of a full-blown "Red Team", or sub-group, that would operate on both a formal and ad hoc basis and participate in IW Fleet Exercises (both as the protector and aggressor), IW-D stand-downs (e.g., a polymorphic virus hits a Navy computer network and immediate action is required), IW-D malpractice (when network monitoring shows events occurring outside the normal operating parameters), and IW-D investigations (system crashes, etc.).

5.9.1.5 Recognize Success

Establish an awards system similar to the Navy Aviation Safety Awards. A key tenant of the naval operation is the recognition of the squadrons and commanders who are successful beyond the norm. The "E" for Excellence is awarded for operational excellence in many areas. Commanders and staff recognize the importance safety plays in this award. Separate awards are also given for safety. IW-D excellence could be recognized as a significant portion of one of the existing awards, or a separate award or trophy could be given to outstanding units.

5.9.1.6 Coordinated Training

Redouble the efforts in bringing everyone involved in Naval automated information systems (sysops, system administrators, CSSOs, etc.) up-to-speed on their role in IW-D. Security, like safety, depends upon the actions of every man and woman in the Navy. Accordingly, the IW community could develop a training program similar to that evolved by the Safety Program. There are some 2,000 specially-trained Safety Officers in the Fleet today. Although the number of networks, sysops, system administrators or AISSOs supporting the Information Warfare community is unknown, the number is probably considerably higher. Consequently, it is probably impractical to train all of them to the same level of expertise given a Safety Officer, but it may be possible to train an equivalent number of INFOSEC Officers who could serve as the ombudsmen for security throughout the fleet. There are significant costs associated with training, but the aviation community has come to accept this as a part of the cost of doing business. The proper training of sysops, etc., should be addressed the same way.

Currently, no centralized training, similar to the Safety School, exists for the field of Information Warfare. If such courses do exist, they are scattered about in various training curricula, and they are probably neither standardized nor evaluated by independent third party Information Warfare professionals. There is no formal Navy training for system operators (sysops) or system administrators, and very little training for Automated Information System Security Officers (AISSOs) in the area of Information Warfare.

Proper safety training ensures that aviation commands have people who are trained and ready to respond to a mishap. They are trained to ensure that the mishap is properly investigated (i.e., that evidence is collected and preserved, etc.). A properly trained Aviation Safety Officer has a good chance of getting to the bottom line--what caused the mishap. On the computer security side of the house, the CSSO should be trained well enough to work in the areas of contingency planning and disaster recovery. The CSSO, acting as an Information Warfare professional, should be trained well enough to initiate immediate action procedures in case of natural disaster, hacker attack, etc. Nowhere in the Navy is this type of training offered.

The IW community needs to identify all of the IW training currently being provided by the Navy, and to ascertain if the sysops, system administrators and CSSO/AISSOs are being properly trained to handle their roles in IW-D. In the Air Force On-Line Survey study [1995 Vulnerability Assessment of Air Force Networked Computer Systems] published in May 1996, the following findings were discovered in the area of security education, training and awareness:

> System administrators indicated a limited awareness of security. Assessment teams concluded that the training received was insufficient, incomplete or ineffective.
>
> Only 52% of the system administrators had received any kind of security training.
>
> The majority perception from the system administrators (93%) is that their users are aware of their security responsibilities; results discovered in the field disputed this perception.

It should be of considerable interest to the IW community if the above Air Force Vulnerability Assessment could be repeated using Navy assets and resources to ascertain if such vulnerabilities exist within the Department of the Navy (DON) community.

5.9.1.7 Risk Management Program

Develop an effective Risk Management program for Navy INFOSEC (IW-D) which will consider the impact of local risk management decisions on the Navy-wide infrastructure. The Naval Aviation Safety community, as well as the Nuclear Regulatory Commission, the National Institute for Occupational Safety and Health, the aerospace industry and many civilian companies have embraced a concept called risk management to improve their success in dealing with risk. Draft OPNAVINST 3500, Operational Risk Management, establishes safety Operational Risk Management as integral in naval operations, training and planning, at all levels, to optimize operational capability and readiness. The Operational Risk Management process is a decision-making tool used by people at all levels to increase operational effectiveness by anticipating hazards and reducing the potential for loss, thereby increasing the probability of a successful mission. (Note: this draft instruction does not currently address security risk management.)

One concern about the use of Operational Risk Management within the IW-D arena is the inherently subjective nature of risk management. Prudence, experience, judgment, intuition and situational awareness are all part of an effective risk management program. Without a long-term commitment and proper foundation in IW-D, there can be no one capable of determining or managing such risk. One would tend to believe that an Information Warfare Officer would need to become a subspecialty designator and the Information Warfare Specialist an enlisted rating within the Navy.

However, any Information Warfare Defense program should still consider implementing some form of an Operational Risk Management technique. It must be understood that no automated information network can be 100 percent “hacker-free.” There is risk within IW-D and it does need to be managed. There must be some realistic goal and this goal must be addressed by all concerned. We can not encrypt everything, and we must believe in the trustworthiness of our systems.

There must be a balance between the role that defensive security measures play and the availability of the network to legitimate users. Much like the different levels of security put into place at an airport, based on the actual or perceived threats to the airport resources (e.g., airport, aircraft, the flying public), Information Warfare Defense must be capable of operating within minimum and maximum levels of risks. An example of this risk envelope could be the operating levels set on a firewall. During periods of perceived low-risk, anyone should be allowed to attach files to an e-mail and send it out via the network. As risks increase, there should be a smaller number of users allowed to perform this function. As risks further increase, the byte size of the outgoing files could be kept to a certain level. As risks further increase, you could stop all attachments to e-mail. Risks increase when the number of packets hitting the firewall from the outside increase beyond an acceptable level. Proper training of sysops, system administrators and AISSOs would give them the knowledge needed to set the acceptable levels. Proper training using the operational risk management process would increase their ability to make informed decisions by providing the best baseline of knowledge and experience available.

It has been said that the amount of risk we will take in war is much greater than that we should be willing to take in peace. Applying the Operational Risk Management process has reduced mishaps, lowered costs and provided for more efficient use of resources. Further research into some form of Operational Risk Management within IW-D is warranted. It may be feasible to look at combining the Risk Assessment methodologies used in the Navy computer security regulation OPNAVINST 5239 with that of OPNAVINST 3500.

5.9.2   Conclusions To The Naval Safety Center Study

The recommendations above described ten recommendations where the IW and INFOSEC community can adapt proven management techniques from the Naval Aviation Safety and NATOPS communities. We found the NSC collects many statistics related to aviation safety, but we were unable to learn how this information is used to guide the course of the safety or NATOPS programs. Metrics were used at many levels to show overall safety success and success related to specific aircraft types, operations and operational locations. The NSC has honed the skill of collecting information and analyzing the statistics to search for answers. The staff at the NSC were very clear of their role of providing service to their fleet customers.

The study team has concluded that there is significant learning potential for the IW community in the analysis of the Naval Air Safety and NATOPS programs. The ten recommendations above identified specific areas where additional study is merited. It was clear to the study team that the aviation and NATOPS communities have clearly defined their goals, adapted a helpful attitude of providing service to their customers, and were willing to have their success, and setbacks, held up for all to see and evaluate. As a result, the safety community has continued to receive the necessary support to manage their programs.

6. IN CONCLUSION--A COMPREHENSIVE SET OF COMMON BEST PRACTICES

This Appendix to the main NDIA C3I study report focused on four major studies in the area of "best practices" in the Information Assurance field. This Appendix provided the reader with a synopsis of:

Commercial Best Practices in the General Arena: The Organization for Economic Cooperation and Development's (OECD) *Guidelines for the Security of Information Systems*

Government Best Practices in the General Arena: A National Institute of Standards and Technology (NIST) report entitled *Generally Accepted Principles and Practices for Securing Information Technology Systems*, dated September 1996.

Commercial Best Practices in a Specific Arena: A United States General Accounting Office (GAO) Report entitled *Information Security Management: Learning From Leading Organizations*, dated May 1998.

Government Best Practices in a Specific Arena: The Report on *The Analysis of the Naval Safety Center as a Model for Information Warfare*, dated January 1997.

There are similar and consistent "best practices" threaded through these four documents. An initial attempt was made in tabular format to provide the reader with these "best practice" similarities. It is hoped that additional time and effort may one day be expended to follow through with a more formal study on these similarities. A new organization formed in the area of Information Assurance would greatly benefit from a more detailed study on "best practices" for its unique mission.

Table 3. "Best Practice" Similarities Between the Four Documents Reviewed

BEST Practices	OECD Guidelines	NIST Report	GAO Report	Naval Safety Center Study
Management	Computer security is an integral element of sound management	Computer security is an integral element of sound management	Establish A Central Management Focal Point	IW-D must evolve a role that works effectively to assist the operational commanders without usurping their authority.
Government Mission	N/A	Computer security supports the mission of the organization	N/A	A security program that views the operational commanders as "customers" may be the only program that can hope to achieve the same level of acceptance that has been attained by the Safety Program.
Responsibilities and Accountabilities	The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.	Computer security responsibilities and accountability should be made explicit	Hold program and business managers accountable	Redouble the efforts in bringing everyone involved in Naval automated information systems up-to-speed on their role in IW-D.

Table 3. "Best Practice" Similarities Between the Four Documents Reviewed (Continued)

BEST Practices	OECD Guidelines	NIST Report	GAO Report	Naval Safety Center Study
Collect Metrics	Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....	Computer security should be cost-effective; computer security should be periodically reassessed.	Monitor factors that affect risk and indicate security effectiveness; Use results to direct future efforts and hold managers accountable; Be alert to new monitoring tools and techniques	Conduct rigorous, non-attribution analysis of significant incidents and provide responsive feedback to the Fleet; Collect and analyze metrics.
Manage and Assess Risk	Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....	Computer security is constrained by societal factors that impacts risks.	Recognize information resources as essential organizational assets; Develop practical risk assessment procedures that link security to business needs; Manage risk on a continuing basis	Availability of accurate and timely threat and vulnerability information could help the Navy fleet-support-contractor team in achievement of Navy goals; Develop and effective risk management program for Navy IW-D.
Training and Awareness	Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.	Computer security requires a comprehensive and integrated approach (includes a discussion on training)	Continually educate users and others on risks and related policies; Use attention-getting and user-friendly techniques	Elevating the visibility of IW-D within the Navy to a level comparable to that of Safety could provide the necessary access.

Table 3. "Best Practice" Similarities Between the Four Documents Reviewed (Continued)

BEST Practices	OECD Guidelines	NIST Report	GAO Report	Naval Safety Center Study
Systems and Policies Integration Approach	Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.	Computer security requires a comprehensive and integrated approach; systems owners have security responsibilities outside their own organizations.	Link policies to business risks; Distinguish between policies and guidelines; Support policies through central security group	Foster a role of assistance rather than one of enforcement.
Internal Assessment	The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.	Computer security should be periodically reassessed.	Assess risk and determine needs	Establish an awards system similar to the Navy Aviation Safety Awards Program.

Best Practices To Solve Network Security Problems

Compiled by
The Carnegie Mellon Software Engineering Institute CERT Coordination Center.

2. Ensure that the software used to examine systems has not been compromised
3. Look for unexpected changes to directories and files
4. Inspect your system and network logs
5. Review notifications from system and network monitoring mechanisms
6. Inspect processes for unexpected behavior
7. Investigate unauthorized hardware attached to your organization’s network
8. Look for signs of unauthorized access to physical resources
9. Review reports by users and external contacts about suspicious system and network events and behavior
10. Include explicit security requirements when selecting server and host technologies
11. Isolate the web server from your organization’s internet network
12. Maintain authoritative copy of your Web site content on a more secure host
13. Offer only essential services and operating system services on the server host machine
14. Consider the security implications when choosing external programs that the server can execute
15. Administer the web server in a secure manner
16. Configure the web server to enhance security
17. Specify security requirements and assess contractor capability
18. Determine contractor ability to comply with your organization’s security policy
19. Require that the contractor software is installed and configured to operate securely
20. Require that the contractor communicate securely with your site when operating remotely
21. Control contractor access to your systems
22. Review contractor performance
23. Eliminate physical and electronic access by the contractor to your systems and networks
24. Develop a computer deployment plan that includes security issues
25. Keep operating systems and applications software up to date
26. Configure computers for user authentication
27. Configure computer operating systems with appropriate object, device, and file access controls
28. Configure network service clients to enhance security
29. Configure computers for file backups

30. Protect computers from viruses and similar programmed threats
31. Develop and promulgate an acceptable use policy for workstations
32. Configure multiple computers using a tested model configuration and a secure replication procedure
33. Allow only appropriate physical access to computers
34. Configure computers to provide only selected network services
35. Establish a policy and set of procedures that prepare your organization to detect signs of intrusion
36. Identify and enable system and network logging mechanisms
37. Identify and install tools that aid in detecting signs of intrusion
38. Generate information required to verify the integrity of your systems and data
39. Establish policies and procedures for responding to intrusions
40. Prepare to respond to intrusions
41. Analyze all available information to characterize an intrusion
42. Communicate with all parties that need to be made aware of an intrusion and its progress
43. Collect and protect information associated with an intrusion
44. Apply short-term solutions to contain an intrusion
45. Eliminate all means of intruder access
46. Return systems to normal operation
47. Identify and implement security lessons learned
48. Design the firewall system
49. Acquire firewall hardware and software
50. Acquire firewall documentation, training, and support
51. Install firewall hardware and software
52. Configure IP routing
53. Identify and enable system and network logging mechanisms
54. Configure firewall packet filtering
55. Configure firewall logging and alert mechanisms
56. Test the firewall system
57. Install the firewall system

58. Configure computers for secure remote administration

59. Phase the firewall system into operation

Best Practices For Software Development Projects

Compiled by
The Software Program Managers Network

60. Formal Risk Management

The discipline of risk management is vital to the success of any software effort. A formal risk management process requires corporate acceptance of risk as a major consideration for software program management, commitment of program resources, and formal methods for identifying, monitoring, and managing risk.

39. Agreement on Interfaces

To deal with the chronic problem of vague, inaccurate and untestable specification, the Council proposed that a baseline use interface must be agreed upon before the beginning of implementation activities, and that such user interface must be made and maintained as an integral part of the system specification. For those projects developing both hardware and software, a separate software specification must be written with an explicit and complete interface description.

40. Formal Inspections

Inspections should be conducted on requirements, architecture, designs at all levels (particularly detailed design), on code prior to unit test, and on test plans.

41. Metric-Based Scheduling and Management

Statistical quality control and schedules should be maintained. This requires early calculation of size metrics, projection of costs and schedules from empirical patterns, and tracking of project status through the use of captured result metrics. Use of a parametric analyzer or other automated projection tool is also recommended.

42. Binary Quality Gates at the Inch-Pebble Level

Completion of each task in the lowest-level activity network needs to be defined by an objective binary indication. These completion events should be in the form of gates that assess either the quality of the products produced, or the adequacy and completeness of the finished process. Gates may take the form of technical reviews, completion of a specific set of tests which integrate or qualify software components, demonstrations, or project audits. The binary indication is meeting a predefined performance standard (e.g., defect density of less than four per function point). Activities are closed only upon satisfying the standard, with no partial credit given. Quality gates can be applied at any time during the project--- including solicitation.

43. Program-Wide Visibility of Progress vs. Plan

The core indicators of project health or dysfunction---the Control Panel indicators---should be made readily available to all project participants. Anonymous channel feedback should be encouraged to enable unfavorable news to move freely up and down project hierarchy.

44. Defect Tracking Against Quality Targets

Defects should be tracked formally at each project phase or activity. Configuration management (CM) enables each defect to be recorded and traced through to removal. In this approach there is no such thing as a private defect, that is, one detected and removed without being recorded. Initial quality targets (expressed, for example, in defects per function point) as well as to counts defects removed in order to track progress during testing activities.

45. Configuration Management

    The discipline of CM is vital to the success of any software effort. CM is an integrated process for identifying, documenting, monitoring, evaluating, controlling, and approving all changes made during the life-cycle of the program for information that is shared by more than one individual or organization.

46. People-Aware Management Accountability

    Management must be accountable for staffing qualified people (those with domain knowledge and similar experience in previously successful projects) as well as for fostering an environment conducive to high morale and low voluntary staff turnover.

Best Practices In Managing World Wide Web Server Security

Compiled by
The Department of Energy (DOE) Computer Incident Advisory Capability (CIAC)

61. Place your web server(s) in a DMZ. Set your firewall to drop connection to your web server on all ports but http (port 80) or https (port 443).

62. Remove all unneeded services from your web server, keeping FTP (but only if you need it) and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.

63. Disallow all remote administration unless it is done using a one-time password or an encrypted link.

64. Limit the number of persons having administrator or root level access.

65. Log all user activity and maintain those logs either in an encrypted form on the web server or store them on a separate machine on your Internet.

66. Monitor system logs regularly for any suspicious activity. Install some trap macros to watch for attacks on the server (such as the PHF attack). Create macros that run every hour or so that would check to integrity of password and other critical files. When the macros detect an change, they should send an e-mail to the system manager.

67. Remove ALL unnecessary files such as phf from the scripts directory /cgi-bin.

68. Remove the "default" document trees that are shipped with Web servers such as IIS and ExAir.

69. Apply all relevant security patches as soon as they are announced.

70. If you must use a GUI interface at the console, remove the command that automatically start the window manger from the .RC startup directories and then create a startup command for the window manger. You can then use the window manager when you need to work on the system, but shut it down when you are done. Do not leave the window manager running for any extended length of time.

71. If the machine must be administered remotely, require that a secure capability such as secure shell is used to make a secure connection. Do no allow.

72. Run the web server in a chroot-ed part of the directory tree so it cannot access the real system files.

73. Run the anonymous FT server (if you need it) in a chroot-ed part of the directory tree that is different from the web server's tree.

74. Do all updates from your Intranet. Maintain your web page originals on a server on your Intranet and make all changes and updates here; then "push" these updates to the public server through an SSL connection. If you do this on a hourly basis, you can avoid having a corrupted server exposed for a long period of time.

75. Scan your web server periodically with tools like ISS or nmap to look for vulnerabilities.

76. Have intrusion detection software monitor the connections to the server. Set the detector to alarm on known exploits and suspicious activities and to capture these sessions for

review. This information can help you recover from an intrusion and strengthen your defenses.

Networks Best Practices Performance Indicators

Compiled by
Booz • Allen Hamilton

	PERFORMANCE INDICATORS		
Security Services	**Minimum Essential**	**Due Care**	**World-Class**
Identification & Authentication			
Identification and Authentication	A unique userid and password combination is required for access to system resources.	A unique userid and password combination is required for access to system resources. All passwords are aged and numerous invalid access attempts deactivate the account. Userid/password, or challenge/response techniques are used in combination with a centralized authentication mechanism such as RADIUS, TACACS, RACF, ACF2, or TSS.	A unique userid and password combination is required for access to system resources. Numerous invalid access attempts deactivate the account. Access is controlled centrally for all resources via a single sign-on architecture. Advanced authentication mechanisms are deployed organization-wide using token-based or biometric devices. Systems incompatible with SSO technology are protected via best due care practices
Access Control			
Router	A minimally-restrictive packet filtering firewall is deployed at all external network gateways.	An integrated firewall is deployed at all external gateways that implements a combination of packet filtering, proxy services, and circuit relay mechanisms. Some application-layer service protections offered. Network address translation is enabled. All non-essential network services are disabled.	An integrated firewall is deployed at all external gateways that implements a combination of packet filtering, proxy services, and circuit relay mechanisms. Network address translation is enabled. All non-essential network services are disabled. Interior firewalls are deployed at strategic points to protect sensitive data and services. All firewalls are centrally controlled by an integrated security management application. Virtual private network(VPN) connections are offered for dial-in users.
File Access	Access to files is restricted based upon user profile and roles.	Access to files is restricted based upon user profile and roles. Access to data is restricted based on individual identify and specific file activities (e.g., read/write vs. read only).	Access to files is restricted based upon user profile and roles. Access to data is restricted based on individual identity and specific file activities (e.g., read/write vs. read only). Access is further restricted by specific data types (e.g., financial, legislative, administrative)
Network Audit and Intrusion Detection	The system collects limited security related activities, and stores them in a protected file for review by security administrators.	Integrated network and host audit and intrusion detection systems implemented behind all external gateways and other critical resources. Comprehensive scanning against full attack profiles implemented, consistent with organization's security policies. Administrators automatically notified of anomalous activities.	Integrated network and host audit and intrusion detection systems implemented behind all external gateways and other critical resources. These systems are integrated with enterprise security management consoles providing central management of security posture. Comprehensive scanning against full attack profiles implemented on all networks, consistent with organization's security policies. Administrators automatically notified of anomalous activities. Enterprise security management tool triggers an automated response to mitigate risks until administrator can manually review.
Confidentiality			

	PERFORMANCE INDICATORS		
Security Services	**Minimum Essential**	**Due Care**	**World-Class**
File-level Encryption	Commercial encryption and security products are available to employees processing or storing sensitive data on their systems.	The enterprise establishes a baseline public key infrastructure, based on a contract with a commercial certificates authority. The enterprise issues certificates to all employees, and a standard commercial crypto tool set is established for employees and IT staff.	The enterprise establishes a comprehensive public key infrastructure, based on its own certificate authority. The enterprise established linkages between certificate authority and directory services on the network. The enterprise issues certificates to all employees with a plan for key recovery. A standard commercial crypto tool set is established for employees and IT staff to encrypt all files available on network resources. Custom applications are developed as needed to support legacy applications.
Transmission Encryption	Commercial encryption and security products are available to employees communicating sensitive data across the network.	The enterprise establishes a baseline public key infrastructure, based on a contract with a commercial certificate authority. Wide spread encryption of traffic eon the enterprise network backbone is established. Key end users systems are equipped with network encryption software and/or hardware and trained in its use.	The enterprise establishes a comprehensive public key infrastructure. Full-scale encryption of all traffic on the enterprise network backbone is established. The enterprise establishes linkages between certificate authority and directory services on the network. All end users systems are equipped with network encryption software and/or hardware and trained in its use.
Integrity			
Non-Repudiation	Individuals within the enterprise allowed to use digital signature based upon commercial certificates (e.g., Verisign).	The enterprise establishes a contract with a commercial certificate authority and issues certificates to all interested employees. Employees are encouraged to use digital signature on all official electronic correspondence and other core business transactions.	The enterprise establishes its own certificate authority and issues certificates to all employees. The enterprise establishes linkages between certificate authority and directory services on the network. Employees are encouraged to use digital signature son all electronic correspondence and other core business transactions.
Data Integrity	All critical data will be protected from modification during storage and electronic transmission.	All critical data will be protected from modification during transmission. Ensure Cyclic Redundancy Checks (CRC) and/or data parity checks are performed on all files being stored and transmitted electronically.	All critical data will be protected from modification during transmission. Ensure Cyclic Redundancy Checks (CRC) and/or data parity checks are performed on all files being stored and transmitted electronically. Archives are electronically time-stamped and digitally signed by a cognizant authority.
Electronic Record Archive	Key financial and business records are archived on a regular basis pursuant to legal and business objectives.	All business records are archived on a regular basis, including financial systems data, accounting data, payroll and human resource data, marketing and sales data, and electronic mail. Archives are stored off site and protected like other critical business records.	All business record are archived on a regular basis by an automated process. These business records include financial systems data, accounting data, payroll and human resource data, and electronic mail. Archives are electronically time-stamped and digitally signed by a cognizant authority. Archives are stored off site and protected like other critical business records.
Availability			

	PERFORMANCE INDICATORS		
Security Services	**Minimum Essential**	**Due Care**	**World-Class**
Disaster Recovery Plan	A comprehensive disaster recovery plan (to include emergency response, contingency, and continuity of operations planning) is developed and all key stakeholders are provided copies.	A comprehensive disaster recovery plan (to include emergency response, contingency, and continuity of operations planning) is developed and all key stakeholders are provided copies. This plan is exercised on an annual basis with core staff.	A comprehensive disaster recovery plan is developed and all key stakeholders are provided copies. This plan is exercised on an annual basis with core staff. Hot site, warm site, or other restoration facilities are procured and incorporated into disaster recovery plans.
Data Backups	Critical data from central servers and databases are backed up to removable storage media on a routine basis. Backup media is rotated, and one set of media is always off site.	Critical data from all network devices are backed up to removable storage media on a routine basis. Backup media is rotated, and one set of media is always off site. Users are provided resources and guidance on backing up personal computers and other end-users equipment.	A comprehensive, centrally-managed backup strategy is implemented enterprise-wide. Critical data from all network devices are backed up to removable storage media on a daily basis. Backup media is rotated, and one set of media is always off site. End-user data is backup to a central facility.
Incident Response Plan	Enterprise-wide plan for responding to network incidents is developed and provided to management and key employees.	Enterprise-wide plan for responding to network incidents is developed. Training is developed and provided to management and key employees on effective incident response. Liaison with state, local, and federal law enforcement offices is established.	An internal computer incident response team is established. Enterprise-wide plan for responding to network incidents is developed. Training is developed and provided to management and key employees on effective incident response. Key non-technical stakeholders, such as public affairs and finance/budget are involved. Liaison with state, local, and federal law enforcement offices is established.
Malicious Code Protection			
User-Level Malicious Code Protection	Mandatory use of commercial anti-virus product on all computers. Periodic updates to the virus signature files are available.	Mandatory use of a commercial anti-virus product on all computers; including real-time scanning of system, e-mail messages, internet downloads, and database accesses. Periodic updates to the virus signature files are available.	Mandatory use of a commercial anti-virus product on all computers; including real-time scanning of system, e-mail messages, internet downloads, and database accesses. Periodic updates to the virus signature files are available. Protection mechanisms for hostile mobile code (e.g., Java, ActiveX) are implemented.
Enterprise-wide Malicious Code Protection	This capability limited to distributing updated virus signature files to multiple platforms and operating systems on a periodic basis.	Enterprise-wide management of anti-virus products is implemented, including the installation of virus signature files periodic updates. Automated scheduling, alerting, and domain management are key features. Support for multiple platforms and operating systems is provided.	Enterprise-wide management of malicious code attacks is implemented. Implementations are centrally controlled and monitored. Scanning for hostile code within e-mail messages and web content is implement at the network level and is invisible to users. Support for multiple platforms and operating systems is provided.
Physical Security			
Physical Access To Server/Communications Systems	All computer rooms, wiring closets, vertical riser spaces, and other related facilities remain locked at all times. Key or push-button locks on all doors.	All computer rooms, wiring closets, vertical riser spaces, and other related facilities remain locked at all times. Key or push-button locks on all doors. Doors equipped with automatic closing and locking mechanisms.	All computer rooms, wiring closets, vertical riser spaces, and other related facilities remain locked at all times. Electronic locks keyed via employee proximity badges or biometric sensors on all doors. Logs of all entries and exits maintained electronically. Doors equipped with automatic closing and locking mechanisms.

	PERFORMANCE INDICATORS		
Security Services	**Minimum Essential**	**Due Care**	**World-Class**
Anti-theft Measures	Database of barcodes and S/N is developed and maintained by security department. Security personnel are trained to question anyone carrying equipment for the premises.	Database of barcodes and S/N is developed and maintained by security department. Security personnel are trained to question anyone carrying equipment form the premises. All mobile computing resources (e.g., laptop computers) are protected by boot-up passwords and/or file encryption.	Database of barcodes and S/N is developed and maintained by security department. Security personnel are trained to question anyone carrying equipment from the premises. Electronic property tags are attached to all computing assets, sensors identify and log all tagged assets as they pass through ingress and egress points
Security Administration			
Risk Assessment	Risk assessment studies are performed prior to initial installation of new hardware, operating systems, and applications, and after significant architectural changes to the network structure.	Risk assessment studies are performed prior to initial installation of new hardware, operating systems, and applications, and after significant architectural changes to the network structure. Risk assessment studies are performed on a regular (e.g., annual) basis, with focused assessments performed after all major network architecture and infrastructure changes.	Risk assessment is an ongoing activity that is tightly integrated with existing enterprise security management tools and enterprise security management tools and enterprise security policies. Regular, routine risk assessments are used to support budgeting and technical decision processes with a focus on maintaining the enterprise's desired security posture.
Vulnerability Scans	Vulnerability scans are run against critical and sensitive systems on a periodic basis.	Vulnerability scans are run against all backbone network components, servers, and critical systems on a continual basis. Multiple scan results are correlated to discover interrelated problems.	Vulnerability scans are run against all network components, including end-user systems on a continual basis. Multiple scan results are stored in a common database to provide centralized control over scan configurations and reporting. Scans are correlated to discover interrelated problems. Results of scans are prioritized to allow administrators to address the most important vulnerabilities first. Rescanning of repaired system is full automated.
Security Policy	An enterprise-wide security policy is in place that reflects management's position on an acceptable security posture.	An enterprise-wide security policy is in place that reflects management's position on an acceptable security posture. This policy is translated into specific security guidelines and procedures which are implemented across the enterprise.	An enterprise-wide security policy is in place that reflects management's position on an acceptable security posture. This policy is translate into specific security guidelines and procedures which are implemented across the enterprise. The security policy is fully integrated into the enterprise management system to allow for seamless, centralized implementation of policy decisions across the IT infrastructure.

APPENDIX C

Examples Of Information Assurance Tools

TABLE OF CONTENTS

1. NETWORK SECURITY AUDITING TOOLS

1.1 Scanning Tools

Asmodeus (Web Trends Corporation)

COPS (Public domain)

CyberCop Scanner (Formerly SNI's "Ballista") (Network Associates)

Internet Scanner (ISS Group, Inc.)

ISS (This tool was created by the same individual who stared ISS Group. It was greatly enhanced and offered as the commercial product "Internet Scanner" mentioned above.) (Public domain)

SATAN (System Administration Tool for Analyzing Networks) (Public Domain)

STAT (Security Test and Analysis Tool) (Harris Corporation)

1.2 Network Intrusion Detection Systems (IDS)

CyberCop Network (Network Associates)

Kane Security Monitor (Intrusion Detection, Inc.)

Net Ranger (Cisco (formerly Wheelgroup))

OmniGuard/ITA (Axent Technologies, Inc.)

RealSecure (ISS Group, Inc.)

SessionWall-3 (AbirNet part of MEMCO)

Stake Out (Harris Corporation)

2. ANTI-VIRUS TOOLS

Name	Company	URL
Adinf	Dialogue Science	http://www.dials.ru
Antigen 5 for Lotus Notes	Sybari	hhtp://www.sybari.com
Antigen 5 for Microsoft Exchange	Sybari	hhtp://www.sybari.com
Antiviral Toolkit Pro	Kaspersky Labs	hhtp://www.avp.ru
AVAST	Securenet	http://www.securenet.org
AVG Anti-Virus System	Grisoft	http://www.grisoft.com
Command Antivirus	Command Software Systems, Inc	http://www.commandcom.com
DiskNet	Reflex Magnetics	http://www.reflex-magnetics.co.uk
DisQuick Diskettes	OverByte Corporation	http://www.disquick.com
Dr. Solomon's Anti-Virus Toolkit	Network Associates, Inc.	http://www.nai.com
Dr. Web	Dialogue Science	http://www.dials.ru
EMD Armor	EMD Enterprises	http://www.emdent.com
ESafe Protect Enterprise	Esafe Technologies	http://www.esafe.com
ESafe Protect Gateway	Esafe Technologies	http://www.esafe.com
F-Secure Anti-Virus	Data Fellows	http://www.datafellows.com
InDefense	Tegam, International	http://www.indefense.com
InoculateIT	Computer Associates	http://www.cai.com/cheyenne
Integrity Master	Stiller Research	http://www.stiller.com
Invircible	NetZ Computing	http://www.invircible.com
IriS AntiVirus Plus	IRiS Antivirus	http://www.irisav.com
McAfee VirusScan	Network Associates, Inc.	http://www.nai.com

Name	Company	URL
MIMEsweeper	Content Technologies, Inc.	http://www.mimesweeper.com
NetShieldNT	Network Associates, Inc.	http://www.nai.com
NOD-iCE	ESET	http://www.eset.sk
Norman Virus Control	Norman Data Defense Systems	http://www.norman.com
Norton Anti-Virus	Symantec Corporation	http://www.symantec.com
OfficeScan	Trend Micro	http://www.antivirus.com
Panda Antivirus	Panda Software	http://www.pandasoftware.com
PC ScanMaster for VINES	Netpro	http://www.netpro.com
Protector Plus	For Windows 95/98, Netware, and NT	http://www.pspl.com
Quick Heal	Cat Computer Services	http://www.quickheal.com
ResQProf	NetZ Computing	http://www.invircible.com
Server ScanMaster for VINES & NT	Netpro	http://www.netpro.com
ServerProtect	Trend Micro	http://www.antivirus.com
Sophos Sweep	Sophos Software	http://www.sophos.com
System Boot Areas Anti-Virus & Crash Recovery	SBABR	http://www.sbabr.com
ThunderBYTE	Norman Data Defense Systems	http://www.norman.com
V-find Security Toolkit	Cybersoft	http://www.cyber.com
VET Anti-Virus	VET Anti-Virus Software Pty LTD	http://www.vet.com.au
Virus ALERT	Look Software	http://www.look.com
VirusBuster	Leprechaun Software	http://www.leprechaun.com.au
VirusNet LAN	Safetynet	http://www.safetynet.com
VirusNet PC	Safteynet	http://www.safetynet.com
Wave Anti-Virus	Cybersoft	http://www.cyber.com

3. SECURITY TOOLS

Network Monitoring Tools

1. Argus
2. Swatch

- Authentication/Password Tools

1. Crack
2. Shadow passwords

- Service-Filtering Tools

1. TCP/IP wrapper program

- Tools to Scan Hosts for Known Vulnerabilities

1. ISS (Internet Security Scanner)
2. SATAN (Security Administrator Tool for Analyzing Networks)

- Multi-Purpose Tools

1. COPS (Computer Oracle and Password System

- Integrity-Checking Tools

1. MD5
2. Tripwire

APPENDIX D

Excerpts From The Report Of Defense Science Board Task Force On Information Warfare-Defense (IW-D), November 1996

TABLE OF CONTENTS

1. RECOMMENDATIONS….

1.1 Assess IW-D Readiness

Information warfare defense should be viewed from a warfighting perspective. Operational forces should be able to detect, differentiate among, warn of, respond to, and recover from disruptions of supporting information services. Recovery from disruptions resulting from failures or attacks might involve repair, reconstitution, or the employment of reserve assets. In some cases, network managers may have to isolate portions of the network, including users of the network, to preclude the spread of disruption. Given the speed with which disruptions can propagate through networks, these capabilities may need to be available in automated form within the network itself. Finally, there must be some means to manage and control these capabilities. At its heart, this is an operational readiness matter.

A standardized process to enable commanders to assess and report their operational readiness status as it relates to their specific dependency on information and information services is an essential element of operational readiness. A standard vocabulary will enable common description of risk scenarios and assessment methodologies. (A more complete explanation of the proposed process is at Appendix C.) The use of a structured assessment and reporting process will help move information assurance from a global and unsolvable problem to the identification of discrete information and information service dependencies that illuminate quantifiable risk to specific information dependent activities within a commander's sphere of responsibility. A similar assessment and reporting process can be applied by supporting elements and in the commercial sector.

Exhibit 6-6 shows that information warfare (defense) must be mainstreamed as a readiness issue. A means must be developed for including information warfare (defense) issues in readiness reporting and a process must be developed to assess the information warfare (defense) readiness posture independently. The assessment scenarios differ from the threat conditions discussed earlier in that the assessment scenarios are used to assess readiness against a wide range of possible threats to specific units, missions, and functions, while the threat conditions are used to describe to existing threat condition to the broad interconnected population. The assessment scenarios are applied locally, while the threat conditions are applied globally. Standardized assessment scenarios could be used for planning considerations, in warning orders and so on. The assessment regime provides a means for addressing variability and should be used in concept and operations planning.

1.1.1 Readiness Assessment System

Need explicit process to tie IW-D readiness assessments to the ability to execute operational missions

Propose standardized, graduated assessment scenarios

Accident

Amateur hackers

Experience hackers

Well-funded non-state purchase of hire of advance IW capabilities

State-sponsored IW

State-sponsored IW with the active collusion of an insider

- Proposed standardized, graduated assessment regime

An unknown information assurance capability for a specified threat scenario

Engineering estimate based on design parameters and recovery plans

Engineering estimate based on design, simulation exercises, and review of recovery plan, but no physical testing for a specified threat scenario

Internal assessment organization and live contingency plan exercise

Independent security assessment organization a live contingency plan exercise

1.1.2 Action

Establish a standard IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies (CJCS lead)

1.2 Readiness Reporting System

Need a standard IW-D preparedness reporting system using assessment factors from previous exhibit

1.2.1 Action

Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example (CJCS lead):

SORTS (Status of Resources and Training System), Joint Pub 1-03.3

- Add IW preparedness to overall unit readiness rating (C-Level)

CSPAR (CINCs Preparedness Assessment Report), Joint Pub 1-03.31

- Add explicit review of IW to review of Ops/Con Plans

CSAAS (Combat Support Agency Assessment System), Joint Pub 1-03.32.1

- Address IW preparedness in new annual CSAAS cycle

Joint Tactisc, Techniques, and Procedures for Base Defense, Joint Pub 3-10.1

- Include IW, apply to CONUS and OCONUS bases

Joint Doctrine to Operations Security, Joint Pub 3-54

- Add IW posture to assessment factors

DISA Communications Spot & Status Reports, Joint Pub 1-03.10

- Modify to include status reporting on major computing resources
- Include CSAs, MilDeps and Service mobilization & sustainment assets

The Task Force recommends that the Chairman of the Joint Chiefs of Staff incorporated information warfare preparedness assessments in the Joint Reporting System and into Joint Doctrine. The systems, reports and publications cited are only examples that the Task Force reviewed to illustrate how these assessments might be incorporated. Additional details will be provided in the written report.

1.3 Appendix C. A Taxonomy For Information Warfare?

…Joint Publication 1-03, "Joint Reporting Structure (JRS)," establishes a standard reporting vocabulary for the Department of Defense. Joint Publication 1-03.3 establishes the "Status of Resources and Training System (SORTS)", and provides the general provisions and detailed instructions for collecting and preparing data on units of the U.S. Armed Forces and selected foreign and international organizations. In practice, the utility of SORTS is not optimum because of the timeliness and quality of data submitted. Whether incorporated in SORTS or a stand-alone method, an information warfare SORTS-like reporting scheme is needed.

SORTS functions as the following:

Central Registry of all Operational Units in the U.S. Armed Forces. SORTS is the single, automated reporting system within the Department of Defense that provides the National Command Authorities (NCA) and the Chairman of the Joint Chiefs of Staff with authoritative identification, location, assignment, personnel, and equipment data for the registered units and organizations of the U.S. Armed Forces, Defense agencies, and certain foreign and international organizations involved in operations with U.S. Armed Forces. The composite registry of all units is maintained by the Joint Staff. After initial registration, SORTS is designed to receive reports by exception when changes occur.

Repository of Resource Status of Selected Units. For selected registered units, SORTS also provides the condition and level of resources and training. This includes the unit commander's assessment of how resources and training levels will affect the unit's ability to undertake its wartime mission. Units report by exception within 24 hours of a change or as directed by the Chairman of the Joint Chiefs of Staff. If no change is unit status occurs within 30 days of report submission, units submit a validation report.

SORTS contains provisions for reporting various readiness items:

Overall C-Level (OVERALL) Set. Data in this set include the overall C-Level for the unit and the codes for primary, secondary, and tertiary degradation reasons. The overall readiness showing how well the unit meets prescribed levels of personnel, equipment, and training for the wartime mission for which the unit has been organized or designed is ranked in descending order from C-1 to C-5:

C-1. The unit possesses the required resources and is trained to undertake the full wartime mission(s) for which it is organized or designed. The resource and training area status will neither limit flexibility in methods for mission accomplishment nor increase vulnerability of unit personnel and equipment. The unit does not require any compensation for deficiencies.

C-2. The unit possesses the required resources and is trained to undertake most of the wartime mission(s) for which it is organized or designed. The resource and training area status may cause isolated decreases in flexibility in methods for mission accomplishment but will not increase vulnerability of the unit under most envisioned operational scenarios. The unit would require little, if any, compensation foe deficiencies.

C-3. The unit possesses the required resources and is trained to undertake many, but not all portions of the wartime mission(s) for which it is organized or designed. The resource and training area status will result in significant decreases in flexibility of mission accomplishment and will increase vulnerability of the unit under many, but not all, envisioned operational scenarios. The unit would require significant compensation for deficiencies.

C-4. The unit requires additional resources or training to undertake its wartime mission(s), but it may be directed to undertake portions of its wartime mission(s) with resources on hand.

C-5. The unit is undergoing a Service-directed resource action and is not prepared, at this time, to undertake the wartime mission(s) for which it is organized or designed.

Personnel Level (PERSONEL) Set. Data in this set include the personnel level (P-level) and a code for the primary reason for degradation in the personnel area.

Equipment and Supplies On Hand Level (EQSUPPLY) Set. Data in this set include the equipment and supplies on hand level (S-level) and a code for the primary reason for degradation in the equipment and supplies on hand area.

Equipment Condition Level (EQCONDN) Set. Data in this set include the equipment condition level (R-level) and a code for the primary reason for degradation in the equipment condition area.

Training Level (TRAINING) Set. Data in this set include the training level (T-level) and a code for the primary reason for degradation in the training area

Forecasted Category Level (FORECAST) Set. Data in this set include the forecasted C-level for the unit and the date the unit expects to attain the C-level.

Category Level Limitation (CATLIMIT) Set. Data in this set include the imposed maximum C-level for the unit, if any, and the primary resource area causing the limitation.

An additional category should be added to SORTS specifying at what level of assessment scenario the unit is prepared to operate and how this preparedness was assessed using the terminology described earlier.

Joint Pub 1-03.10, "JRS Communications Status," provides for the Defense Information Systems Agency to provide near-real-time status information on a serious degradation of the Defense Communication System (DCS) via a Communications Spot Report and to provide a summary of significant status information on the DCS via a daily Communications Status Report.

These reports should be expanded to include information systems and information services. Further, these reports should be used by the military departments, services, combat support agencies and the CINCs to report the status of information systems and services.

Joint Pub 1-03.31, "Preparedness Evaluation System," establishes the CINCs Preparedness Assessment Report (CSPAR). These report provide a biennial appraisal of the preparedness of the unified and specified commands to accomplish Joint Strategic Capability Plan tasks (both supporting and supported) within the constraints of the total apportioned force (Active and Reserve). In the CSPAR, each CINC identifies overall strengths and significant deficiencies affecting the command's ability to carry out assigned missions and execute the plans produced during the most recent planning cycle. In submitting the CSPAR, CINCs are reporting on their ability to accomplish a specific task using available capabilities.

The CINCs should be required to include an assessment of their ability to carry out assigned missions at the appropriate assessment scenario level and indicate the process used to determine preparedness.

Joint Pub 1-03.32.1. "Combat Agency Assessment System," sets forth the guidelines and procedures for operating the Combat Support Agency Assessment System (CSAAS), a uniform system for reporting to the Security of Defense, the commanders of the unified and specified commands (CINCs), and the Secretaries of the Military Department concerning readiness of each combat support agency to perform with respect to a war or threat to national security.

Chairman, Joint Chief of Staff (CJCS)-sponsored exercises provide the principal means of on-site evaluation of agency responsiveness in reacting to National Command Authority decisions and CINC warfighting requirements. In the event no such exercises are scheduled during the first two quarters of even-numbered fiscal years, Joint Staff observers conduct independent site visits to each of the combat support agencies. Although the CSPAR is the principal means for the combatant commands to assess agency support, Joint Staff observers may also visit combatant command headquarters to discuss overall support, agency supporting plans, and ongoing efforts to improve shortfalls.

These reports should be modified to include an annual assessment of the preparedness of the combat support agencies, at a specified assessment level to carry out their mission. The current two year schedule currently followed in assessing the readiness of combat support agencies is not realistic in a age of information warfare. The information dependent process of these agencies are directly tied to the ability to mobilize, deploy and sustain the forces. Currently, this is an unknown in the age of information warfare.

Joint Pub 3-10.1, "Joint Tactics, Techniques, and Procedures for Base Defense," categorizes threats to bases in the rear area by the levels of defense required to counter them. Emphasis on specific base defense and security measures may depend on the anticipated threat level. (These threat levels are discussed detail in Joint Pub 3-10.)

Level I threats can be defeated by base or base duster self-defense measures.

Level II threats are beyond base or base cluster self-defense capabilities but can be defeated by response forces, normally military police (MP) units assigned to area commands with supporting fires.

Level III threats necessitate the command decision to commit a Theater Contingency Force. Level III threats, in addition to major ground attacks, include major attacks by aircraft and theater missiles armed with conventional weapons or nuclear, biological and chemical (NBC) weapons.

The threat to bases in the rear area should be modified to include information warfare attacks.

Joint Pub 3-10.1 also spells out Threat Conditions and Responses and states that in combating terrorism, bases should use common terrorist threat conditions (THREATCONs), each with its specific security measures and required responses.

Threat assessments are used to determine threat levels, to implement security decisions, and to establish awareness and resident training requirements. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors:

Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity.

History. Demonstrated terrorist activity over time.

Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.

Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to implement their intentions.

The severity of the terrorist threat is indicated by the designated threat level, assigned through analysis of the above threat assessment factors. Threat levels, and associated factors, are:

Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

High. Factors of existence, capability, history and intentions must be present.

Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

Low. Existence and capability must be present. History may or may not be present.

Negligible. Existence and/or capability may or may not be present.

The terrorist threat level is one of several factors used in the determination of terrorist THREAT CON. Factors that enter into the decision to assign a particular THREATCON and its associated measures include threat, target vulnerability, criticality of assets, security resource availability, impact on operations and morale, damage control, recovery procedures, international regulations, and planned U.S. Government actions that could trigger a terrorist response.

The terrorist THREATCON system provides a common framework to facilitate inter-Service coordination, support U.S. military anti-terrorist activities, and enhance overall DOD implementation of U.S. Government anti-terrorist policy. THREATCONs are described below:

THREATCON NORMAL. Applies when a general threat possible terrorist activity exist, but the threat warrants a routine security posture.

THREATCON ALPHA. Applies when there is a general threat of terrorist activity against personnel and installations, the exact nature and extent of which are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO measures. However, base defense forces may have to implement selected measures from higher THREATCONs based on intelligence received. Base defense forces must be able to maintain the measures in this THREATCON indefinitely.

THREATCON BRAVO. Applies when an increased and more predictable threat of terrorist activity exists. Base defense forces must be able to maintain the measures of this THREATCON for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

THREATCON CHARLIE. Applies when an incident occurs or when intelligence indicates an imminent terrorist action against U.S. bases and personnel. Implementation of measures in the THREATCON for more than a short period probably will create hardship and affect peacetime activities of the unit and its personnel. Sustaining this posture for an extended period probably will require augmentation.

THREATCON DELTA. Applied in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

The description of threat levels, threat assessments, severity of threat, and threat condition found in Joint Pub 3-10.1 is a good model for information warfare defense preparation, assessment, and warning.

Finally, Joint Pub 3-54, "Joint Doctrine for Operations Security," Change 1, Appendix E, outlines procedures for Operations Security (OPSEC). Theses surveys in general:

Thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.

Check on how effective the OPSEC measures the operation or activity being surveyed in protecting its critical information.

Cannot be conducted until after an operation or activity has at least identified its critical information for without a basis of identified critical information, there can be no specific determination that actual OPSEC vulnerabilities exist. (This is also true in information warfare.)

Each OPSEC survey is unique. Surveys differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the activity to be surveyed

In combat, a survey's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that will permit the adversary to counter friendly operations or reduce their effectiveness.

In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary's long-rang planning.

OPSEC Surveys are not Security Inspections:

OPSEC surveys are different from security evaluations or inspections. A survey attempts to produce an adversary's view of the operation or activity being surveyed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

Surveys are always planned and conducted by the organization responsible for the operation or activity that is to be surveyed. Inspections may be conducted without warning by outside organizations.

OPSEC surveys are not a check on the effectiveness of an organization's security program or its adherence to security directives. In fact, survey teams will be seeking to determine if any security measures are crating OPSEC indicators. …Surveys are not punitive inspections, and no grades or evaluations are awarded as a result of them. Surveys are not designed to inspect individuals but are employed to evaluate operations and systems used to accomplish missions.

To obtain accurate information, a survey team must depend on positive cooperation and assistance from the organizations participating in the operation or activity being surveyed. If team members must question individuals, observe activities, and otherwise gather data during the course of the survey, they will inevitable appear as inspectors, unless this non-punitive objective is made clear.

Although reports are not provided to the surveyed unit's higher headquarters, OPSEC survey teams may forward to senior officials the lessons learned on a non-attribution basis. The senior officials responsible for the operation or activity then decide to further disseminate the survey's lessons learned.

There are two basic kinds of OPSEC surveys: command and formal.

A command survey is performed using only command personnel and on events within the particular command

A formal survey requires a survey team composed of members form inside and outside the command and will normally cross command lines (after prior coordination) to survey supporting and related operations and activities

Both types of surveys follow the same basic sequence and procedures.

Although Joint Pub 3-54 is scheduled to be rewritten, it is quoted extensively as another possible model for conducting information warfare assessments. The assessment methodology cited at the beginning of the annex should yield more rigorous conclusions.

By adopting concepts from each of the Joint Pub sources cited above a standard vocabulary of status reporting, tied to specific information dependent processes, can be developed for information warfare. Such as assessment and reporting system should be developed that stands on its own for use in civil agencies and the commercial sector. Within the Department of Defense this may be more easily achieved by making suitable modification of the several portions of the Joint Reporting System.

In the case of information warfare, as in the terrorism example above, a range of standardized threat scenarios should be promulgated for use in conducting preparedness surveys, as standardized assessment conditions for planning purposes, and a set of standardized threat warning or THREATCONS, if warning is available.

Whatever schema is used to evaluate the operational readiness of information dependent processes and activities, it must be timely and reflect the current state of the security policy being implemented, the supporting infrastructures (computers, communications, electricity and other supporting utilities) and the training status of the personnel, both systems administrator and users of information and information systems.

APPENDIX E

Red Team Evaluation and Acceptance Criteria

TABLE OF CONTENTS

1. RED TEAM EVALUATION AND ACCEPTANCE CRITERIA

[NOTE: Evaluation Criteria is for the Certification of the TEAM, NOT of the system. Each COMPANY should have basic entry criteria. Personnel should have minimal entry criteria. Performance metrics should be maintained on both Company and Personnel participants.]

1.1 Background

This NDIA IA study has identified a need to establish evaluation and acceptance criteria for companies and teams identified as possible candidates for performance of outsource activities involved in Red Team Testing and Certification of DOD information systems. This study has taken this process one step farther by establishing evaluation and acceptance criteria for the Red Team Testing and Certification process itself. To meet this need, this appendix will present a high level overview of the envisioned criteria for Company participation, Personnel [Team Membership] participation, and Red Team Testing Process evaluation and acceptance criteria.

1.2 Company Evaluation And Acceptance Criteria

Individual companies must be selected in advance for consideration as valid participants in the outsourcing process.

Since the overall purpose is to provide a mediated [pseudo] attack on sensitive and/or classified DOD information systems, the primary consideration must be ownership of the company. The first criteria in the qualification process, therefore, would indicate restriction to U. S. owned companies.

Since Red Team activities are representative of attacks carried out in a planned scenario at a predefined and coordinated time and place, company participation should be restricted to those companies with a demonstrated ability to perform government contracting successfully. The demonstrated ability of a company to provide quality, timely, cost-effective services based on past performance of the company should be a key selection factor.

Red Team activities are both planned and crisis-driven. Consequently, the proven ability of a company to respond successfully to surge tasking, as demonstrated in a company's past performance, must be a selection factor.

Concern is often expressed with the need to maintain consistency in the Red Team membership, avoiding unnecessary or frequent personnel changes during extended activities or periods of performance. Preferential selection should be based on the employee turnover rating of individual companies.

Red Team tactics generally assume an adversary's ability to employ both current and emerging technologies and tactics. Company selection should consider the commitment that the company has in maintaining the technical capabilities of employees through internal and external training programs, continuing education opportunities, and professional development programs. Likewise, Government must make a concerted effort to ensure that companies have access to requisite training for task performance, training which might have previously been restricted to Government or "preferred" contractors.

Company participation must consider the technical ability of the company to understand the issues and tactics employed. Consequently, selection should take into consideration the company involvement in DOD activities, service level activities, information technology activities, and system type activities. The selected companies should have a positive history of involvement in all appropriate areas.

In keeping with the generally accepted principle of Red Team activities as being completely independent, impartial, and unbiased as feasible, company selection for specific tasking should ensure that the company has not been involved in the procurement, design, development, implementation, or testing of the specific target program, platform, or system(s). Company involvement must consider activities as Prime contractor, subcontractor, and consultancy roles.

The last two items on company evaluation and acceptance criteria present a significant difficulty in the selection process. A company must be involved in related activities, but not for the target agency, platform, or system being tested. However, that implies that a company might inadvertently gain access to proprietary or business sensitive information produced or developed by a primary competitor. This risk must be fully evaluated.

1.3 Personnel [Red Team Member] Evaluation And Acceptance Criteria

As with companies, each individual selected to participate in Red Team Testing activities must also be selected in advance for consideration as valid participants in the outsourcing process. Selection of individual team membership is, in theory, much easier than selection of a company. As with the selection criteria for participation in a major design or development activity, specific Labor Categories and qualifications within the Labor Categories must be identified, providing the ability to select a well rounded team with all of the requisite skills to perform necessary Red Team activities. Generally speaking, no one person will have the skills necessary to perform Red Team testing unless the specific test is very limited in size and scope.

Individuals selected should be U. S. Citizens.

Individuals selected must have or be able to obtain the appropriate security clearances for the specific tasking under consideration.

Individuals selected must have extensive experience with DOD Information Technology [years determined by level of expertise required].

Individuals selected should have experience with the agency or agencies being supported.

Individuals selected must have experience with the CLASS of systems being targeted.

Individuals selected, in limited situations, will need to have specific hands-on experience with a given system.

Individuals selected must have been pre-screened for deployment suitability [medical, dental, financial, psychological].

Individuals selected must have been qualified for one or more Labor Category descriptions deemed necessary to support the overall Red Team Testing and Certification program.

Individuals selected should have hands-on familiarity with the tools, processes, or practices appropriate for the specific Labor Category task performance.

Individuals selected must meet the predefined educational/professional/experience level qualifications for the specific Labor Category or Categories. Generally, years of experience should be an acceptable substitute for degree requirements. Likewise, professional certifications, such as Certified Information Systems Security Professional (CISSP), should be an acceptable substitute for degree requirements.

Individuals selected should have a demonstrated history of successful job performance in a DOD Information Technology environment.

1.4 Process Evaluation And Acceptance Criteria

The Red Team Testing and Certification process, as with the company and team membership selection process, must be subjected to evaluation and acceptance criteria to be deemed a viable program. The Red Team Testing program is a phased or segmented process; consequently, the evaluation and acceptance of that process should also be phased or segmented. The traditional phased structure is generally accepted to be pre-event, event, and post-event. We do recognize that the pre-event phase is occasionally subdivided, in that overall program planning and specific target attack planning are separate activities. Further, the specific target attack planning must fall within the parameters of the overall program planning guidelines.

1.4.1 Pre-event Phase

Program Planning - Program planning establishes the overall purpose, composition, and objectives of the Red Team Testing and Certification program.

Program planning must be supportive of the current directives, policies, and requirements levied upon [and by] the DOD.

Program planning must have a clearly defined set of overall program goals.

Program planning goals must have a clearly defined set of metrics to gauge goal accomplishment.

Program planning must establish a description of services to be provided [Red Team Testing without Blue Team support; Red Team Testing with Blue Team support; Follow-on On-site Training; Follow-on On-site Security Remediation; Follow-on System Owner Remediation].

Program planning must identify the organizational structure of the program office, to include staff billets and chain of authority.

Program planning for staff billets must establish Labor Categories and Job Descriptions for Government, civilian, and contract billets.

Program planning must establish security clearance requirements for program participation.

Program planning must establish boundaries and constraints for program activities.

Program planning must establish oversight responsibilities and procedures.

Program planning must establish sources of data gathering.

Program planning must establish points of contact for specific agency interaction.

Program planning must establish processes and procedures for requesting services acceptable to serviced agencies.

Program planning must establish reporting criteria and procedures, to include serviced agencies, systems owners, and OSD.

Specific Target Attack Planning

Evaluation Criteria:

- **Considerations:**
  - **Directives/Policy/Requirements**
  - **Sensitivity Analysis**
    - **Security**
    - **Privacy**
    - **Legal**
    - **Contractual**

Evaluate/Acceptance:

- **Pre-event**
  - **Data Collection**

NOTE: Data Collection is for System Specifications. Evaluation and acceptance of the system is already established. The system requirements should be contained in:

  -
    - **System Specifications**
    - **Functional Requirements**
    - **Interface Specifications**
    - **Security Requirements**
    - **Documentation**
    - **Training Requirements**
    - **Concept of Operations [CONOPS]**
    - **Security Concept of Operations [SECONOPS]**
    - **Operational Requirements**
    - **Security Policy**
  - **Boundaries Definition [Rules of Engagement]**
  - **Establish the Team**
    - **Certification of Team**
    - **Training of Team**
  - **Test and Evaluation Review**
- **Event**
  - **Continue Data Collection**
  - **Modify [if/as needed] the Rules of Engagement [ROE]**
- **Post Event**
  - **Evaluation/Acceptance**
    - **Based upon Red Team Reports**
  - **Report Goes to:**
    - **Owner of the System**
    - **OSD Coordination Office**
    - **DIAP [Defense Information Assurance Process]**

Red Team does event, provides report.

Sanitized Report - remove names of personnel, etc. - goes to OSD

Full Report on system goes to system owner.

Owner has actions to decide what gets fixed.

OSD Coordination Office does follow-ups.

Certification Criteria and Training

Best Practices [Government and Industry]

Standardization [same for all - CinC/Svc/Agency]

Current Processes

Current OSD Policy

Issues

2. TESTING AND VALIDATION PROCEDURES.

As this task has evolved during the study, testing and validation procedures now relate to two areas:

Testing and validation of any required certification process for the personnel participating in Red Team exercises; and

Testing and validation of the Red Team process itself.

Item (1) will be addressed first. Any certification process, where individuals are trained and tested in specific skills before receiving certification to perform some task, requires the following minimal validation activities:

Evaluation, and periodic re-evaluation, of the categories of certification by existing experts in the field to ensure that the categories of certification represent appropriate partitioning of the required expertise.

Examination, and periodic re-examination, of the certification requirements by existing experts in the field to ensure that the requirements are complete, current, appropriate, and achievable.

Periodic examination of a sample of recently certified personnel by independent experts, to ensure that the certification process has sufficient rigor.

Collection of feedback from certified personnel regarding recommended changes to the certification process.

A continuing education program and a re-certification process for certified personnel, to reflect the changing information and technology involved in the specialty.

Collection and analysis of appropriate metrics on the certification process (% enrollees that receive certification, distribution of the number of unsuccessful attempts to receive certification, etc.) to ensure that an appropriate and cost effective certification program remains in place.

Because of the rapid changes in the technology and information available in this field, special attention must be placed on selecting the appropriate timeframes for all of the periodic activities listed above. It is recommended that the minimal acceptable period would be annual, and the maximum would will be two years.

Item (2), the testing and validation of the Red Team process itself, is a much more difficult task.

Red Teams are customarily prohibited from performing a large number of activities (often either illegal or damaging to property or information) that could easily be performed by actual hostile personnel attempting to compromise an information system. In many cases, assessing the validity of a Red Team result involves the subjective assessment of the relative importance of actions that the Red Team was not allowed to take. It is this area, the assessment, application, control, review, and approval of Red Team constraints and permissions that must be addressed for any validation of the Red Team process. Specific issues to be addressed include:

Realism of the attack.

Effects of notification on the results of the effort.

Assessment of the attack level of sophistication relative to intelligence estimates of the capabilities of potential adversaries.

Enumeration and realistic assessment of the probable effects of prohibited Red Team activities (and “missed opportunities” deriving thereof during the exercise).

Where Red Team exercises are conducted in a laboratory environment, realistic extrapolation of the laboratory environment to the real environment.

It is anticipated that evaluation criteria related to the above issues could be prepared for each of the major classes and types of Red Team efforts. These evaluation criteria could be used to establish a ‘realism’ assessment of any Red team action and be used as an additional tool in evaluating the results of a Red Team.

APPENDIX F

Red Team Life Cycle Management

TABLE OF CONTENTS

1. LIFE CYCLE MANAGEMENT

We have developed a "typical Red Team Outsourcing Life Cycle" that is threaded through a Red Team Process. We used the Defense-wide Information Assurance Red Team (D-IART) methodology process as the guideline to mirror and process-drive the outsourcing life cycle. The resultant life cycle is based on six chronologically related phases that facilitate our (and others') understanding of the process. The phases are:

I. Government Planning Phase - 24 to 12 months in advance of actual event

II. Event Planning Phase – 11 to 6 months in advance of actual event

III. Mission Planning Phase – 5 to 0 months in advance of actual event

IV. Operations Phase – plus 1 to 6 months

V. Post Operations Phase – plus 7 to 9 months

VI. Interim Phase – between specific operations

Each phase has a core of activities and may have fringe activities that tie into the core of another phase.

Phase I is Government Policy and Guidance. Phase 1 centers on Government's lead actions to fund, guide, and operate the Red Team. It has been generally agreed that these activities are not likely to be outsourced. In the event they are outsourced it is the consensus that any company contracted to assist the Government in Phase 1 activities should normally be excluded by reason of conflict of interest from participating in competition for related subsequent Government contracts.

Phase II involves actual event planning. The details of the event are planned out, assignments made, and primary players, locations, and limits are delineated. The Statement of Work would be written during this period, security requirements identified, and the actual domain or footprint of the event would be sketched out. This is phase during which data will be compiled, developed and modeled for both for system(s) and threat. A strawman mission plan will be developed during this phase.

Phase III builds on previous phases and delves into the technical aspects of what will actually transpire during the event. The mission plan is finalized, allowable tactics are identified and focus will be drawn on specific "targets". All team members will be identified by name, assignments made, and structure, roles, and responsibilities will be finely tuned. More detailed actions include developing the balance between exploitation and training, acceptable levels of intrusiveness and disruption (if applicable), teams will be identified. Scripting will be developed and actual Blue benefits should be developed in full during this phase.

During Phase IV the event takes place. All forces in previous phases are brought to bear to ensure objectives are met during event execution. Phase V is the end game marked by such events as wrap-up reports, lessons learned, populating technical and historic data bases for the use of future teams. During Phase VI the Red Team members train and prepare for future events.

The following is an outline of the Red Team process cycle. Phase I is primarily items a through k below.

I. Phase I

a. Execution Plan. The Government will develop and promulgate the heart of the impending event through a Concept of Operations (CONOPS). The CONOPS will delineate the core information for the event that includes naming identifying commands, dates of the event(s), objective(s), and providing specific assignments.

b. Budget. Budget activities may occur as far as two years in advance beginning with budget estimate summaries and continuing through execution years. Because budget is at the heart of any contracted events it is important that budgets be well established in advance and remain stable to preclude erratic hire and fire situations.

c. Security (DD-254). The Government will develop and promulgate security requirements. These requirements are anticipated to run the entire length of the spectrum, to include special programs requiring polygraphs.

d. Limits. The Government will establish limits that ensure safety for Red Team employees. Specific attention was focused on efforts that may be required in or near hostile areas.

e. Threat Data. Threat data can be a constantly changing element and will be directly related to each separate system or set of systems (systemic relationships). The Government needs to ensure that threat data is consistently identified in a timely manner, tracked, catalogued and categorized for Red Team use.

f. System Data. The Government will develop target system data to include most recent updates, software patches, for the Red Team's use. System data will be the Red Team's core information through which it will develop its strategy and evaluate options.

g. Red Team Rules of Engagement (ROE). The Government will develop the Red Team Rules of Engagement. The ROE will feature the limits, rules, intentional boundaries, and establish set points for required Red Team notifications and actions.

h. Owner Buy-In. The command owning the target system needs to be a willing and unthreatened party to the Red Team event. Willing "targets" will be much more receptive to Red Team activities as a necessity to maintain and improve operational readiness.

i. Certifications. The Government may develop minimum, intermediate, and advanced technical credentials for Red Team operators. Credentials may be required for Red Team members and spelled out in procurement documents. It is likely during early stages of developing Red Team outsourcing that credentials will waived and granted on a pending basis until all requirements can be met.

j. Training. This is area where industry feels vulnerable. No credentials have been developed for Red Team members. Government may develop requirements that delineate both credentials and essential skills for Red Team members and for specific Red Team events. The constant technology advances make it too costly for industry to keep personnel abreast of the technology required for the wide range of systems across the DOD. It is anticipated that Government contracts for Red Team services will contain clauses that call for Red Team members who are between assignments to be assigned to training laboratories and classrooms to maintain current skills and to develop new skills.

k. Roles and Responsibilities. The Government will develop and promulgate roles and responsibilities for both Government and contractor performance. General initial statements to this effect will be found in the Request for Proposal and details will be explained in the issuing orders and CONOPS.

l. Industry Request for Proposal (RFP) / Request for Information (RFI), types of contracts and considerations: The Government has several options as spelled out by the FAR when acquiring technical services. The types of contracts are described below with excerpts taken directly from the FAR.

    47. Level of Effort: FAR 16.207-2 -- Level of Effort: Firm-Fixed-Price, Level-of-Effort Term Contracts -- Description. A firm-fixed-price, level-of-effort term contract requires -- (a) The contractor to provide a specified level of effort, over a stated period of time, on work that can be stated only in general terms; and (b) The Government to pay the contractor a fixed dollar amount. A firm-fixed-price, level-of-effort term contract is **suitable for investigation or study** in a specific research and development area. The **product of the contract is usually report showing the**

results achieved through application of the required level of effort. However, payment is based on the effort expended rather than on the results achieved.

48. Cost Plus: FAR 16.305 -- Cost-Plus-Award-Fee Contracts. A cost-plus-award-fee contract is a cost-reimbursement contract that provides for a fee consisting of (a) a base amount (which may be zero) fixed at inception of the contract and (b) an award amount, based upon a judgmental evaluation by the Government, sufficient to provide motivation for excellence in contract performance. Cost-plus-award-fee contracts are covered in Subpart 16.4, Incentive Contracts. 16.306 -- Cost-Plus-Fixed-Fee Contracts. (a) Description. A cost-plus-fixed-fee contract is a cost-reimbursement contract that provides for payment to the contractor of a negotiated fee that is fixed at the inception of the contract. The fixed fee does not vary with actual cost, but may be adjusted as a result of changes in the work to be performed under the contract. This contract type permits contracting for efforts that might otherwise present too great a risk to contractors, but it provides the contractor only a minimum incentive to control costs. Application. (1) A cost-plus-fixed-fee contract is suitable for use when the conditions of (I) The contract is for the performance of research or preliminary exploration or study, and the level of effort required is unknown; or (ii) The contract is for development and test, and using a cost-plus-incentive-fee contract is not practical. (2) A cost-plus-fixed-fee contract normally should not be used in development of major systems (see Part 34) once preliminary exploration, studies, and risk reduction have indicated a high degree of probability that the development is achievable and the Government has established reasonably firm performance objectives and schedules.

49. Time and Materials (T&M): FAR 16.601 -- Time-and-Materials Contracts. (a) Description. A time-and-materials contract provides for acquiring supplies or services on the basis of -- (1) Direct labor hours at specified fixed hourly rates that include wages, overhead, general and administrative expenses, and profit; and (2) Materials at cost, including, if appropriate, material handling costs as part of material costs. (b) Application. A time-and-materials contract may be used only when it is not possible at the time of placing the contract to estimate accurately the extent or duration of the work or to anticipate costs with any reasonable degree of confidence. (1) Government surveillance. A time-and-materials contract provides no positive profit incentive to the contractor for cost control or labor efficiency. Therefore, appropriate Government surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used. (2) Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures consistent with Part 31. (c) Limitations. A time-and-materials contract may be used (1) only after the contracting officer executes a determination and findings that no other contract type is suitable and (2) only if the contract includes a ceiling price that the contractor exceeds at its own risk. The contracting officer shall document the contract file to justify the reasons for and amount of any subsequent change in the ceiling price.

50. Indefinite Delivery/Indefinite Quantity: FAR Subpart 16.5 This subpart prescribes policies and procedures for making awards of indefinite-delivery contracts and establishes a preference scheme for making multiple awards of indefinite-quantity contracts. This subpart does not limit the use of other than competitive procedures authorized by Part 6. Nothing in this subpart shall be construed to limit, impair, or restrict the authority of the General Services Administration (GSA) to enter into schedule, multiple award, or task or delivery order contracts under any other provision of law. Therefore, GSA regulations and the coverage for the Federal Supply Schedule program in Subpart 8.4 and Part 38 take precedence over this subpart. This subpart may be used to acquire information technology requirements that are not satisfied under the Federal Supply Schedule program. Definitions Delivery order contract" means a contract for supplies that does not procure or specify a firm quantity of supplies (other than a minimum or maximum quantity) and that provides for the issuance of orders for the delivery of supplies during the period of the contract. Task order contract" means a contract for services that does not procure or specify a firm quantity of services (other than a minimum or maximum quantity) and that provides for the issuance of orders for the performance of tasks during the period of the contract. General. (a) There are three types of indefinite-delivery contracts: definite-quantity contracts, requirements contracts, and indefinite-quantity contracts. The appropriate type of indefinite-delivery contract may be used to acquire supplies and/or services when the exact times and/or exact quantities of future deliveries are not known at the time of contract award. Pursuant to 10 U.S.C.2304d and section 303K of the Federal Property and Administrative Services Act of 1949, requirements contracts and indefinite-quantity contracts are also known as delivery order contracts or task order contracts. (b) The various types of indefinite-delivery contracts offer the following advantages: (1) All three types permit -- (i) Government stocks to be maintained at minimum levels; and (ii) Direct shipment to users. (2) Indefinite-quantity contracts and requirements contracts also permit -- (i) Flexibility in both quantities and delivery scheduling; and (ii) Ordering of supplies or services after requirements materialize. (3) Indefinite-quantity contracts limit the Government's obligation to the minimum quantity specified in the contract. (4) Requirements contracts may permit faster deliveries when production lead time is involved, because contractors are usually willing to maintain limited stocks when the Government will obtain all of its actual purchase requirements from the contractor.

51. Blanket Purchase Agreement (BPA): FAR 13.303-1 -- General. (a) A blanket purchase agreement (BPA) is a simplified method of filling anticipated repetitive needs for supplies or services by establishing "charge accounts" with qualified sources of supply (see subpart 16.7 for additional coverage of agreements). (b) BPAs should be established for use by an organization responsible for providing supplies for its own operations or for other offices, installations, projects, or functions. Such organizations, for example, may be organized supply points, separate independent or detached field parties, or one-person posts or activities.

    FAR 3.303-2 -- Establishment of BPAs. (a) The following are circumstances under which contracting officers may establish BPAs: (1) There is a wide variety of items in a broad class of supplies or services that are generally purchased, but the exact items, quantities, and delivery requirements are not known in advance and may vary considerably. (2) There is a need to provide commercial sources of supply for one or more offices or projects in a given area that do not have or need authority to purchase otherwise. (3) The use of this procedure would avoid the writing of numerous purchase orders. (4) There is no existing requirements contract for the same supply or service that the contracting activity is required to use. (b) After determining a BPA would be advantageous, contracting officers shall -- (1) Establish the parameters to limit purchases to individual items or commodity groups or classes, or permit the supplier to furnish unlimited supplies or services; and (2) Consider suppliers whose past performance has shown them to be dependable, who offer quality supplies or services at consistently lower prices, and who have provided numerous purchases at or below the simplified acquisition threshold. c) BPAs may be established with –

(1) More than one supplier for supplies or services of the same type to provide maximum practicable competition; (2) A single firm from which numerous individual purchases at or below the simplified acquisition threshold will likely be made in a given period; or (3) Federal Supply Schedule contractors, if not inconsistent with the terms of the applicable schedule contract.

52. Classified: Classified contracts may be awarded through appropriate agencies. The accesses required to complete Red Team tasks may limit industry's ability to respond to Government's requirements. This is particularly true if sporadic tasking becomes the rule rather than the exception.

53. Liability: Industry's concerns focus on individual and corporate liability. In general, liability levels commensurate with those levied on Government employees is acceptable. Because of the wide range of liability possibilities associated with Red Team activities, industry requires strong language to indemnify in the instance of unintentional harm or damage.

54. Other Key Clauses:
    a. Non-Disclosure
    b. Key Personnel
    c. Conflict of Interest
    d. Constraints/Limits
    e. Termination Clause

9. Who Can Participate?

    a. Reserves. Red Teams offer a superb opportunity for reserve personnel to participate. Using this intellectual capital resident within the reserves brings a wealth of talent to the Red Team's table for a minimal investment. In the long haul the aggregate of reserve personnel who attain Red Team experience will serve to increase overall operational readiness.

    b. Government Labs. These facilities and FFRDCs are prime candidates to provide hardware and software benches to conduct research, trend analysis, and predictive analyses in support of Red Team tasks

c. Educational Institutions. Same benefits seen here as in the Government labs. The major benefit with the educational institutions is the youthful population who possesses superior computer skills.

d. Profit, Nonprofit Labs. Brings additional talent to the problem.

m. Red Team Events. Red Team events and tasks that involve Red Team members occur during Phase II – Phase VI.

1. Detail Test Plan (Phase II – III)

a. Roles, responsibilities, structure

1. Red Team
2. Blue Team
3. White Team
4. Advisory Panel

b. Timeline

c. Bounds

d. Assets

5. Personnel
6. Skills required
7. Equipment
8. Related logistics

e. Expected outcome

9. Benefits to Blue
10. Benefits DOD-wide, systems, components

f. Approvals

g. Facilities/Resources

h. Script (Concept/CONOPS)

i. Record keeping

j. Contingency / Escape / Recovery Plan

2. Conduct Actual Red Team Event (Phase IV)

n. Report (Phase V)

3. Distribution

4. Security

a. At least as high or higher than system being evaluated
b. Multiple classifications depending upon level of detail

3. Sanitized

b. No names
c. Non-attribution

4. Recommendations (viewed as a possibility for industry)

a. Substantive
b. Offer solution(s)

5. Timeliness

a. Hot wash-up for immediate feedback to Blue
b. Operationally critical information fed back in near real-time

6. Lessons Learned
a. Red Team lessons
b. White Team lessons
c. Blue Team lessons
d. Not necessarily shared amongst teams

o. Follow-up (Government Function) (Phase VI)

1. Risk assessment
2. Potential solutions
3. Cost Benefit Analysis of implementing potential solutions
4. Budget process
5. Implementing change(s)
6. Standardizing the Red Team process
7. Trend analysis
a. Red Team data
b. Build Red Team data base
a. Technical
b. Process
c. Problems Vs solutions
8. Training
a. For Red Team personnel in between events
b. For others across DOD
c. Feed material into DOD schools

p. End Cycle / Start Over

q. Issues

1. Legal
a. Privacy
b. Consent
c. Trusted agents
d. FOIA
e. Civil rights
f. Jurisdiction
2. Ownership
a. Who owns the target system?
3. Security
a. System
b. Personnel
c. Facility
4. Liability
a. Corporation
b. Government

c. Individual

APPENDIX G

Interview Comments

TABLE OF CONTENTS

1. RESULTS

Although there were the expected differences in view there were also a number of striking patterns. The following is a summary of the key points from those interviews.

1.1 Industrial Support To Red Teaming And Other IA Activities

Most of the interviewees at the higher levels of the organizational chain were very concerned about "outside" participation in Red Teaming and other IA activities. The concern ranged from security issues, to free enterprise and competition issues, to indemnification, liability and other legal and contractual issues. Many of those interviewed agreed that DOD has insufficient talent in these areas but some were very reluctant to agree that outsourcing was the answer. This attitude is not surprising considering the accountability issues at this level.

At the lower level commands where the day to day business of conducting IO/IA activities is a reality, all of the individuals interviewed, stated that they are using contractor support in some if not all of these areas. While the levels and areas of support varied, all respondents agreed that, considering the current manning levels and expertise, it would be virtually impossible to accomplish their missions without contractor support.

1.2 Training

All of the respondents agreed that there is a significant lack of training in the many areas associated with IO/IA and, in fact, there are ongoing effort to alleviate this shortfall.

1.3 Manpower

As we have seen, there seems to be general agreement that there are inadequate quantities of qualified individuals within DOD commands. But, because of the way day-to-day operations are conducted and because IO/IA has evolved within DOD, there is no clear delineation of IO/IA related duties within either the military officer, enlisted or DOD civilian communities. Therefore, it is very difficult to estimate just how many personnel are employed in these areas and how many are required, with what skill base, in order to operate efficiently. This makes it very difficult to even estimate the magnitude of the problem.

2. SPECIFIC COMMENTS FROM INTERVIEWS

DOD doesn't have its IA act together in-house. Trying too much to use its own resources.

Too early to consider outsourcing. We have concern over Command and Control (C2). If we decide to outsource, contractors will do everything except C2 and they will not have overall responsibility.

No one in DOD is looking at this subject by taking into consideration the entire problem.

DOD IA activities are not well coordinated.

Red Team functions should be outsourced in order to gain access to technical skills not available within the military or civilian ranks.

Using contractors depends on the organization and sometimes depends on scalability: Big organizations like the Army are using industry/contractors. Smaller organizations like the Defense Security Service (DSS) use only government resources. Other organizations such as the Joint Warfare Intelligence Center (JWIC) use only Federally Funded Research and Development Centers (FFRDC).

Can contractors offer any other/greater expertise the DOD/National Security Agency (NSA)? Doubt there is a resource problem since NSA is advertising to do these types of activities for government agencies. We should follow NSA guidelines for Red Teams.

We should balance assurance need vs. business strategy. What do Red Teams/Vulnerability Assessments do to operations and budgets? How much is enough to achieve security? How expensive is it for an attacker to get into a system?

Threats and vulnerabilities to DOD information systems are not well understood.

Solutions to mitigate risk might not be technical in nature. Instead we have to be concerned on the trust we place on people. We worry about the threat posed by insiders.

Economic issues are getting people's attention and DOD is more focused on this area. Budgets and personnel resources are declining and there is constant pressure to downsize.

What is the impact of outsourcing on operational readiness? Can outsourcing be a force multiplier? How do we maintain our critical core capabilities? As an example some system administration functions were outsourced and we don't know how to measure the impact. We need tools to predict the impact on operational readiness if certain things happen. If we test every year how do we measure improvements?

Red Teaming functions are being outsourced to the Reserves and this is a cultural shock. The Reserves are acting as Primes with industry contractors acting as subs.

What is the government organization which will satisfy the Joint Chiefs of Staff (JCS)? Who pays for Red Teams and Vulnerability Assessments? Should there be centralized funding for these functions?

Who is worrying about coalition IA?

We foresee big problems if we use contractors for deception and psychological operations functions.

How do we get necessary information to the right people in a timely fashion so they can fix problems? When we don't do this we experience big problems. Who has positive control of a network in order to provide indications of a problem? How do military commanders (CDR) fix things when special handling requirements are involved?

Most military CDRs want military personnel to do Red Teams and Vulnerability Assessments. Big problem is how to train, certify and retain these people?

Pace of technology advancement doesn't allow the DOD to keep pace in-house, especially when it comes to people and training. This is why we must outsource.

DOD IA is harder because of the size of the problem. How much is DOD spending for IA vs. industry? DOD hasn't stepped up to investment requirements for IA. IA is now under funded.

The Joint Task Force is Computer Network Defense (JTF/CND) was/is a stop – gap measure. It was never intended to be all purpose. Rather it was to do essential warfare tasks.

NSA has established some impressive capabilities with regard to IA. They can certify organizations and companies to carry out certain IA related functions. NSA certifies some commercial off-the shelf (COTS) products.

There is no central DOD organization that is aware of what is taking place across all of DOD. What organization is the clearing house for Red Teams? Should it be the Space Command? We need to be able to call a single point of contact to explain certain ongoing activities (like Red Teaming).

Best practices are mostly held very close and it is often too late when we find out about them. We also do not define the threat in a timely manner. DIA reports take too long. Once we know the threat we have to deal with risks and determine the importance of the system.

We can't afford the $ involved to fully test for IA. How do we ensure certification/interoperability across all necessary platforms?

We need DOD an organization whose primary responsibility is to find the best tools/practices to help us with IA.

There is no IA policy for testing Red Teams. Certification of people is a big problem.

We need to model after the Food and Drug Administration – how do they test/monitor/certify?

What is the incentive for industry and the government to work more closely in the IA arena?

We don't have a universally accepted policy to certify contractors. We don't have the capacity to delivery on all requirements being levied on us. As a result we have to turn to contractors to help us out.

The big Red Team in the sky – who coordinates; who controls, who is in charge? How do we handle civil and criminal liability?

We need DOD policy and guidance on IA and Red Teams because people are carrying out Red Team activities every day but they are not all following the same procedures. Policy should be ASD/C3I.

There are no standards for training Red teams. There is no certification for Computer Emergency Response Teams (CERT).

IA isn't a readiness criteria.

When looking at metrics one must consider that certain things can't be measured. For example, how do we measure protection?

DOD doesn't know how many system administrators they have.

We need a definition and taxonomy for tools.

DOD doesn't own most of their systems. They mostly ride on commercial networks.

Number one concern is $ and people.

It is easy to tell why you need a tank – it is tied to a military mission. How do you determine the value of IA if it is not a discreet piece of equipment.

Policy is lagging. Have to understand what is involved. Technology is rapidly changing. Have to get consensus.

This is not a technical problem. It is a management problem.

3. NIDIA INFORMATION ASSURANCE SURVEY QUESTIONNAIRE

NDIA INFORMATION ASSURANCE SURVEY QUESTIONNAIRE

SD - Strongly Disagree
D - Disagree
N - Neutral
A - Agree
SA - Strongly Agree
N/A - Not Applicable

		SD	D	N	A	SA	N/A
1.	**Your organization participates in supporting Information Assurance.**						
a.	Your members participate on red teams.						
b.	There are formal standards for red team performance.						
c.	Your red team has a formal mission (I.e., goal).						
d.	Your red team has established roles and responsibilities.						
e.	Your red team has clearly defined and written functions.						
f.	Your members participate on blue teams.						
g.	Your members participate on blue teams.						
1)	There are formal standards for blue team performance.						
h.	Your members participate on white teams.						
1)	There are formal standards for white team performance.						
i.	You have standing teams vis a vis ad hoc teams.						
j.	Your red team bases its efforts on threat versus vulnerability.						
k.	Red teams are most effective as part of exercises rather than in the context of day-to-day operations.						
2.	**Your red team has a standing organizational structure.**						
a.	Red teams are more effective if they have a standing organization rather than an ad hoc organization.						
b.	There are benefits to having this organizational structure.						
c.	There are detractors in having this organizational structure.						
d.	This structure is preferred to ad hoc teams.						
e.	Your red team is built around an organizational core of technical competency.						
f.	Your red team is built around an ad hoc convening of talents.						
1)	This structure is preferred to standing teams.						
g.	You have the required red team resources to fulfill your mission.						
h.	You would make near-term changes to your red team organization.						
i.	You would make mid-term changes to your red team organization.						
j.	You would make long-term changes to your red team.						
3.	**You use red teams more than once a year.**						
a.	Funding limits your use of red teams.						
b.	Time/schedule limits your use of red teams.						
c.	Qualified personnel limit the use of red teams.						
d.	Other resources limit your use of red teams.						
e.	Boundaries and constraints are placed on red teams.						
f.	Boundaries and constraints are vulnerability based.						
4.	**There are requirements to consider in planning a red team event.**						
a.	Long lead time is a consideration in planning a red team event.						
b.	Red Team events have representative time lines, including durations.						
c.	There are cycles associated with red team planning.						
d.	Your red team events vary in scope.						
e.	Red team events planning requires certain talents and capabilities.						
f.	Your red team planning includes representative milestones.						
5.	**Classifications levels are considerations in planning and executing a red team event.**						
6.	**There are legal and contractual considerations in planning and executing a red team event.**						
a.	Individual rights are an important consideration.						
b.	Contractual considerations may impact a red team event.						
c.	Rules of engagement are essential factors in planning and executing a red team event.						
d.	Liability issues are important factors in planning and executing a red team event.						
7.	**You agree that red team functions could be outsourced.**						
a.	There are benefits to be derived from outsourcing red team functions.						
b.	Some red team functions are being outsourced today.						
c.	There are pieces of the red team that should be outsourced.						
d.	There are pieces of the red team that should not be outsourced.						
e.	Technical competency is a concern to outsourcing red team functions.						
f.	Legal competency is a concern to outsourcing red team functions.						
g.	Process control is a concern to outsourcing red team functions.						
h.	Security and possible disclosure poses concerns to outsourcing red team functions.						
i.	There are other significant concerns and drawbacks to outsourcing red team functions.						
j.	A Government process (that complements downsizing) is needed to effectively manage red team outsourcing.						

NIDIA INFORMATION ASSURANCE SURVEY QUESTIONNAIRE (Continued)

NDIA INFORMATION ASSURANCE SURVEY QUESTIONNAIRE

SD - Strongly Disagree
D - Disagree
N - Neutral
A - Agree
SA - Strongly Agree
N/A - Not Applicable

		SD	D	N	A	SA	N/A
k.	A government organizational structure is needed to effectively manage red team outsourcing.						
l.	Specific tools or other necessary assets need to be made available to the contractor if red team efforts are outsourced.						
8.	**Red team products or deliverables are essential.**						
9.	**The red team report should be brief (20 pages or less).**						
a.	Metrics must be cited in the red team products or deliverables.						
b.	Metrics must be accompanied by measures of effectiveness and/or measures of performance.						
c.	Wide distribution of the final repot is needed to impact operational readiness.						
d.	A constant/consistent effort to define and promulgate best practices is important.						
10.	**Feedback mechanisms are important to support future red team functions.**						
11.	**Your red team activities interact with the NII/DII.**						
12.	**Your red team activities impact systems/components outside of your control.**						
13.	**You would define the most effective red team activities as "no notice attacks".**						
14.	**You would define the most effective red team activities as "cooperative assessments".**						
15.	**You frequently interact with other DoD organizations on matters of Information Assurance.**						
16.	**You interact with organizations external to DoD on matters of Information Assurance.**						
17.	**You interact with organizations external to the federal government on matters of Information Assurance.**						
18.	**This study can benefit red team performance across the DoD.**						

APPENDIX H

References and Links

TABLE OF CONTENTS

1. DOCUMENTS

[CADM, 1997] C^{4}ISR Core Architecture Data Model, Version 1.0, 15 September 1997.

[CAF, 1997] C^{4}ISR Architecture Framework, Version 2, 18 December 1997.

[Campbell, 1997] Campbell, Douglas. Refining the Management of IW-D Plans, Goals, Milestones and Metrics Based on Three Successful Navy Programs. Alexandria, VA: Corbett Technologies, Inc., 1997.

[Cebrowski, 1998] Cebrowski, USN, Vadm Arthur K. ANetwork-Centric Warfare B Its Origin and Future.@ U.S. Naval Institute Proceedings, p. 31, January, 1998.

[CJCSI6212, 1995] CJCS Instruction 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems. Washington, DC: Joint Chiefs, 30 June 1995.

[Clemins, 1998] Clemins USN, ADM Archie. Remarks to AFCEA Asia Pacific TECHNET 98. Asia Pacific TECHNET Conference, Honolulu, HI, 5 Nov 1998.

[DOD4630, 1998] DOD Directive 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C^{3}I) Systems. Washington, DC: Department of Defense, 1998.

[DOD8320, 1998] DOD 8320.1-M-1, Draft DOD Data Element Standardization Procedures, February, 1998.

[DOD 1999] Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense: Initial Report. Washington DC: Office of the Secretary of Defense (OSD) April 1999

[DODI5200, 1997] DOD Instruction 5200.40 DOD Information Technoloogy Security Certification & Accrediation Process (DITSCAP). Washington, DC: Department of Defense, December 1997

[DODI8500.xx 1998] DOD Instruction 8500.xx Draft, Information Assurance Requirements. Washington, DC: Department of Defense, 1998

[DODD8500, 1998] DOD Directive 8500.xx Draft, Informtion Assurance Program. Washington DC: Department of Defense, 1998

[DSBGS, 1993] Report of the Defense Science Board Task Force on Global Surveillance. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, 1993.

[DSBR, 1994] Report of the Defense Science Board Task Force on Readiness. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, June 1994.

[DSBR, 1996] Report of the Defense Science Board Task Force on Information Warfare-Defense. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, November 1996

[GAO, 1998] Joint Military Operations: Weaknesses in DOD's Process for Certifying C^{4}I

[IATAC 1998/1999] IA newsletter Vol 2. No. 3 & 4. Washington, DC: Information Assurance Technology Analysis Center (IATAC) 1998/1999

[ITSG, 1998] Information Technology Standards Guidance B Information Management. Final Draft Version 1.0. Washington, DC: Department of the Navy, 1998.

[JCS, 1997] Information Assurance: Legal, Regulatory, Policy and Organization Considerations, 3rd edition. Washington, DC: Joint Chiefs of Staff (JCS), 1997.

[JCS 1-02] JCS Pub 1-02.

[JCS 1997] Information Warfare: A Strategy for Peace the Decisive Edge in War. Washington, DC: Joint Chief of Staff (JCS), 1997

[JCS 1999] Information Operations: A Strategy for Peace the Decisive Edge in War. Washington, DC: Joint Chief of Staff (JCS), 1999

[JITC, 1998] C^{4}I InteroperabilityBJITC Certification Process. JITC Home Page, 21 Oct 1998.

[JTA, 1996] Department of Defense Joint Technical Architecture, Version 1.0, 22 August 1996.

[JTA, 1997] Department of Defense Joint Technical Architecture, Draft Version 2.0, 18 July 1997.

[SAIC, 1996] Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd edition. McLean, VA: Science Applications International Corporation (SAIC), 1996.

[USD(A&T), 1996] Implementation of the DOD Joint Technical Architecture. USD(A&T) and ASD(C^{3}I) Joint Memorandum. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 1996.

1.1 Other Documents

"OSD Initiatives in Information Assurance," MILCOM 98. Virginia Caston, OASD (C3I)/IA.

"Information Warfare- Defense (IW-D), Acquisition & Implementation Plan Strategies". CAPT C.T. Ristorcelli, 27 Sep 96

"Improving Information Assurance," ASD (C3I), 28 Mar 97

“Defense Reform Initiative Doctrine (DRID) 20 Implementation” OASA (MRA)29 May 98

“C^3I, C^4ISR, Information Superiority” Art Money OASD (C3I), 12 Jan 98

“Best IT Practices in the Federal Government,” C10 Council and Industry Advising Council, Oct 97

“Organization & Business Case Model for Information Security,” SAIC, 26 Aug 97

2. LINKS

http://www.doncio.navy.mil (DON IT Standard Guidance (ITSG))

http://www.info-sec.com/pccip/web/index.html

http://www.sei.cmu.edu/pub/documents/97.reports/pdf/97sr003.pdf

http://www.engarde.com (En Garde Systems)

http://all.net (Fred Cohen & Associates)

http://www.pccip.gov/report_index.html (Marsh Report)

http://www.miora.com (Miora Consulting, Inc)

http://www.research.att.com/~smb/talks/net-inet-sec/sld001.htm http://www.securityexperts.com (The Security Experts)

http://www.ciao.gov (Critical Infrastructure Assurance Office)

http://www.pccip.gov (President's Commission on Critical on Infrastructure Protection)

http://www.odci.gov/cia/public_affairs/speeches/dci_testimony_062498.html

http://www.ciac@llml.gov (DOE’s Computer Incident Advisory Capability (CIAC))

http://www.cio.gov/iac (CIO Industry Advisory Council)

http://www.cert.org (CERT Coordination Center)

http://www.first.org (Forum of Incident Response and Security Teams)

http://www.gocsi.com (Computer Security Institute)

http://www.cs.purdue.edu (Purdue University Computer Sciences Dept)

http://www.iss.net (Internet Security Systems)

http://www.assist@assist.mil (DISA Center for Automated System Security Incident Support Team)

“Critical Foundations: Thinking Differently,” The President’s Commission on Critical Infrastructure Protection

APPENDIX I

Acronyms

TABLE OF CONTENTS

3. ACRONYMS

The following acronyms have been used throughout this report and are included here for reference.

ADR	Anomaly Detection and Reaction
ASAP	As Soon As Possible
CBT	Computer Based Training
CC	Common Criteria
CERT	Computer Emergency Response Team
CIAC	Computer Incident Advisory Capability
CO	Contracting Officer
COI	Conflict of Interest
CONOP	Concept of Operations
COTS	Commercial Off-The-Shelf
CSA	Combat Support Agency
CSIS	Center for Strategic and International Studies
DEPSECDEF	Deputy Secretary of Defense
DIAP	DOD-wide Information Assurance Program
D-IART	Defense Information Assurance Red Team
DII	Defense Information Infrastructure
DIRNSA	Director National Security Agency
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSB	Defense Science Board
EPL	Evaluated Products List
FAR	Federal Acquisition Regulation
GAO	General Accounting Office
GII	Global Information Infrastructure
GSA	General Services Administration
IA	Information Assurance
IAC	Information Assurance Center
IATAC	Information Assurance Technology Analysis Center
IAW	In Accordance With
IDS	Intrusion Detection System
INFOSEC	Information Systems Security
IO	Information Operations
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
IW	Information Warfare
JCS	Joint Chiefs of Staff
JITC	Joint Interoperability Test Command
JMRR	Joint Monthly Readiness Report
NDA	Non-Disclosure Agreement
NDIA	National Defense Industrial Association
NDU	National Defense University
NIAP	National Information Assurance Partnership

NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OASD/C3I	Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
OSD	Office of the Secretary of Defense
PDM	Program Decision Memorandum
PL	Public Law
POA&M	Plan of Action & Milestones
R&D	Research & Development
ROE	Rules of Engagement
ROI	Return on Investment
SOP	Standard Operating Procedure
SORTS	Status of Resources and Training Systems
SOW	Statement of Work
TCSEC	Trusted Computer System Evaluation Criteria
T&E	Test & Evaluation
TPEP	Trusted Product Evaluation Program
TOR	Terms of Reference
TTAP	Trust Technology Assessment Program
USC	United States Code
WBS	Work Breakdown Structure

APPENDIX J

Study Team Membership

TABLE OF CONTENTS

1. STUDY TEAM MEMBERSHIP

Chairman

Fred Demech	TRW

Co-Chairman

Dr. Ray Curts	GRCI & Strategic Consulting
Richard Wilhelm	BAH

Members

Dr. John Alger	ITT & Mitre
Jay Birch	BAH
Kerry Butterfield	Mitre
Dr. Doug Campbell	Syneca Research Gourp
Michelle Check	IMG
Rick Dame	GRCI
Mike Donnell	GWU
Don Fleet	GRCI
Jim Flynn	GRCI
John Flynn	GTE/BBN
Jeff Grover	GTRI
Leo Hart	Mitre
Tom Hart	GRCI
Bill Hingston	TRW
Don LeVINE	TRW
Greg Michaels	GRCI
Celeste Pace	GRCI
Mark Raczynski	GD
Julie Ryan	JRI
Mike Shank	Delfin & FGM
Mary Shupack	TRW
Angelo Spandaro	GRCI
Bob Thompson	BAH
Neil Wagoner	Mitre
Rusty Wall	CSC
Chris Wilson	Harris
Lori Woehler	Sytex & Secure Computing
Owen Wormser	C3I
Bernie Ziegler	SAIC

Members of the Study Legal Panel

Bob Axelrod	Mitre
Harvey Bernstein	CSC
Brian Craig	TRW
Bill Meyers	BAH
Ron Palenski	GTE
Herb Raiche	GRCI

Government Liaison Members

Virginia Castor	OASD/C3I
Gus Guissanie	OASD/C3I

APPENDIX K

Acknowledgements

TABLE OF CONTENTS

2. ACKNOWLEDGEMENTS

Discussions were held with representatives from the following organizations:

Government

Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
The Joint Chiefs of Staff Joint Directorates
Director, Operational Test & Evaluation
National Security Agency
Defense Intelligence Agency
Defense Advanced Research Projects Agency
Defense Information Systems Agency
Defense Security Service
Defense Threat Reduction Agency
Joint Task Force for Computer Network Defense
US Army, Air Force, Navy and Marine Corps
Central Intelligence Agency
Land Information Warfare Activity
Fleet Information Warfare Center
Air Force Warfare Information Center
Space and Naval Warfare Systems Command
Army Digitization Office
Air Force Electronic Systems Command
Joint Interoperability Test Command
National Infrastructure Protection Center
Information Assurance Technology Analysis Center

Industry Companies

Booz • Allen Hamilton
CSC
C3I
Delfin Systems
General Dynamics
GRC International
GTE/BBN
Harris
Information Management Group
ITT Industries
SAIC
Secure Computing
Syneca Research Group
SYTEX
TRW

Other Organizations

Georgia Tech Research Institute
George Washington University
Highlands Forum
Mitre
Potomac Institute for Policy Studies